COMTREND CORPORATION

CT-5611TC
ADSL2+ Combo Router
User's Manual

Version A1.0, July 21, 2008

261070-010

Preface

This manual provides information related to the installation, operation, and application of this device. The individual reading this manual is presumed to have a basic understanding of telecommunications terminology and concepts.

If you find the product to be inoperable or malfunctioning, please contact technical support for immediate service by email at INT-support@comtrend.com

For product update, new product release, manual revision, or software upgrades, please visit our website at http://www.comtrend.com

Important Safety Instructions

With reference to unpacking, installation, use and maintenance of your electronic device, the following basic guidelines are recommended:

- Do not use or install this product near water, to avoid fire or shock hazard. For example, near a bathtub, kitchen sink or laundry tub, or near a swimming pool. Also, do not expose the equipment to rain or damp areas (e.g. a wet basement).
- Do not connect the power supply cord on elevated surfaces. Allow it to lie freely. There should be no obstructions in its path and no heavy items should be placed on the cord. In addition, do not walk on, step on or mistreat the cord.
- Use only the power cord and adapter that are shipped with this device.
- To safeguard the equipment against overheating, make sure that all openings in the unit that offer exposure to air are not blocked.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightening. Also, do not use the telephone to report a gas leak in the vicinity of the leak.
- Never install telephone wiring during stormy weather conditions.

CAUTION:

- To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.
- Always disconnect all telephone lines from the wall outlet before servicing or disassembling this equipment.

WARNING

- Disconnect the power line from the device before servicing.
- Power supply specifications are clearly stated in Appendix B.

Copyright

Copyright©2008 Comtrend Corporation. All rights reserved. The information contained herein is proprietary to Comtrend Corporation. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of Comtrend Corporation.

NOTE:	This document is subject to change without notice.

Protect Our Environment

This symbol indicates that when the equipment has reached the end of its useful life, it must be taken to a recycling centre and processed separate from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this router can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with your household waste. You may be subject to penalties or sanctions under the law. Instead, ask for disposal instructions from your municipal government.

Table of Contents

CHAPTER 1 INTRODUCTION 5

CHAPTER 2 INSTALLATION 6

2.1 HARDWARE INSTALLATION 6
2.2 FRONT PANEL 7
2.3 USB DRIVER AUTORUN INSTALLATION 8
2.4 USB DRIVER MANUAL INSTALLATION (64BIT OS) 10

CHAPTER 3 WEB USER INTERFACE 16

3.1 DEFAULT SETTINGS 16
3.2 IP CONFIGURATION 16
3.3 LOGIN PROCEDURE 18

CHAPTER 4 QUICK SETUP 20

4.1 AUTO QUICK SETUP 20
4.2 MANUAL QUICK SETUP 21
4.2.1 PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE) 22
4.2.2 MAC Encapsulation Routing (MER) 26
4.2.3 IP Over ATM 29
4.2.4 Bridging 32

CHAPTER 5 DEVICE INFORMATION 34

5.1 WAN 35
5.2 STATISTICS 35
5.2.1 LAN Statistics 35
5.2.2 WAN Statistics 36
5.2.3 ATM statistics 37
5.2.4 ADSL Statistics 38
5.3 ROUTE 40
5.4 ARP 41
5.5 DHCP 41

CHAPTER 6 ADVANCED SETUP 42

6.1 WAN 42
6.2 LAN 42
6.3 NAT 44
6.3.1 Virtual Servers 44
6.3.2 Port Triggering 45
6.3.3 DMZ Host 47
6.3.4 ALG 48
6.4 SECURITY 49
6.4.1 IP Filtering 49
6.4.2 MAC Filtering 52
6.4.3 Parental Control 54
6.5 QUALITY OF SERVICE 55
6.6 ROUTING 56
6.6.1 Default Gateway 56
6.6.2 Static Route 57
6.7 DNS 58
6.7.1 DNS Server 58
6.7.2 Dynamic DNS 58
6.8 DSL 60
6.9 CERTIFICATE 61
6.9.1 Local 61
6.9.2 Trusted CA 63

CHAPTER 7 DIAGNOSTICS 65

CHAPTER 8 MANAGEMENT 67

8.1 SETTINGS 67
8.1.1 Backup Settings 67

8.1.2 Update Settings *67*
8.1.3 Restore Default *68*
8.2 SYSTEM LOG 69
8.3 SNMP AGENT 71
8.4 TR-069 CLIENT 71
8.5 INTERNET TIME 72
8.6 ACCESS CONTROL 72
8.6.1 Services *73*
8.6.2 IP Addresses *74*
8.6.3 Passwords *74*
8.7 UPDATE SOFTWARE 75
8.8 SAVE AND REBOOT 76

APPENDIX A: PIN ASSIGNMENTS 77

APPENDIX B: SPECIFICATIONS 78

APPENDIX C: SSH CLIENT 80

APPENDIX D: SECURITY 81

Chapter 1 Introduction

The CT-5611TC ADSL2+ Combo Router provides a 10/100Base-T connection, mini USB interface and ADSL2+ port for high-speed Internet access. It features TR-068 compliant LED indicators and colored rear panel connectors quick installation.

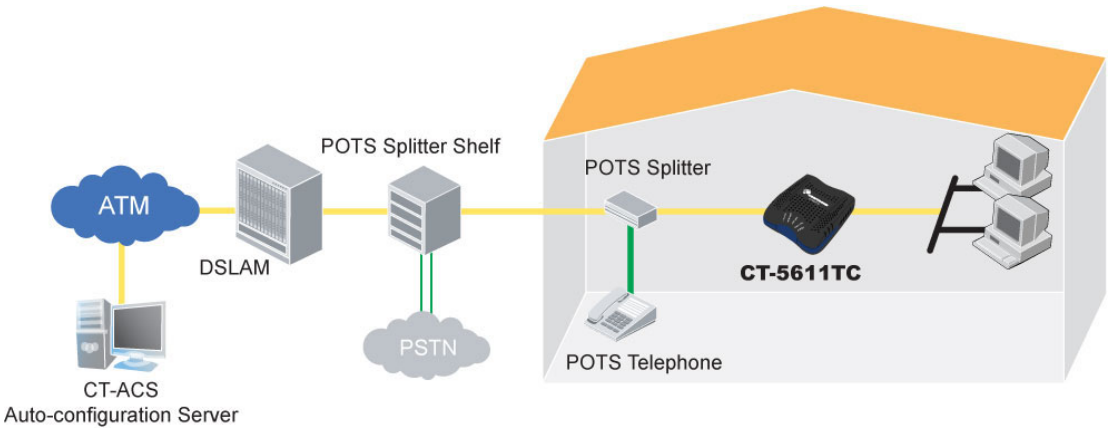
It can achieve data transmission rates of up to 24 Mbps over ordinary telephone lines, which is more than enough speed for Video on Demand. It also has full bridging and routing capabilities with advanced security functions, such as: Firewall, Virtual Private Networks with PPTP pass-through, L2TP pass-through, IPSec passthrough.

FEATURES

- ADSL2+ over POTS (Annex A)
- Dynamic IP assignment
- Auto PVC configuration (up to 8 VCs)
- NAT/PAT
- IP filtering
- SPI (Stateful Packet Inspection)
- DoS protection
- Static route and RIP v1/v2
- IGMP Proxy
- DHCP Server/Relay/Client
- DNS Proxy
- Web-based management
- FTP/TFTP server
- Embedded SNMP agent
- IP/MAC address filtering
- TR-068/TR-069/TR-098/TR-111 standard compliance
- Remote administration, automatic firmware upgrade and configuration, configuration backup and restoration

APPLICATION

The following diagram depicts the application of the CT-5611TC.



Chapter 2 Installation

2.1 Hardware Installation

Follow the instructions below and reference this graphic for hardware setup.

Connection to LINE - If you wish to connect both the router and a telephone, connect the LINE port to a POTS splitter with a RJ11 connection cable.

Connection to LAN
Use RJ45 cable to connect a network hub or PC. The LAN port is auto-sensing MDI/X and either straight-through cable or crossover cable can be used.

Connection to USB
Connect the USB port to a PC with a mini-USB to standard USB cable.

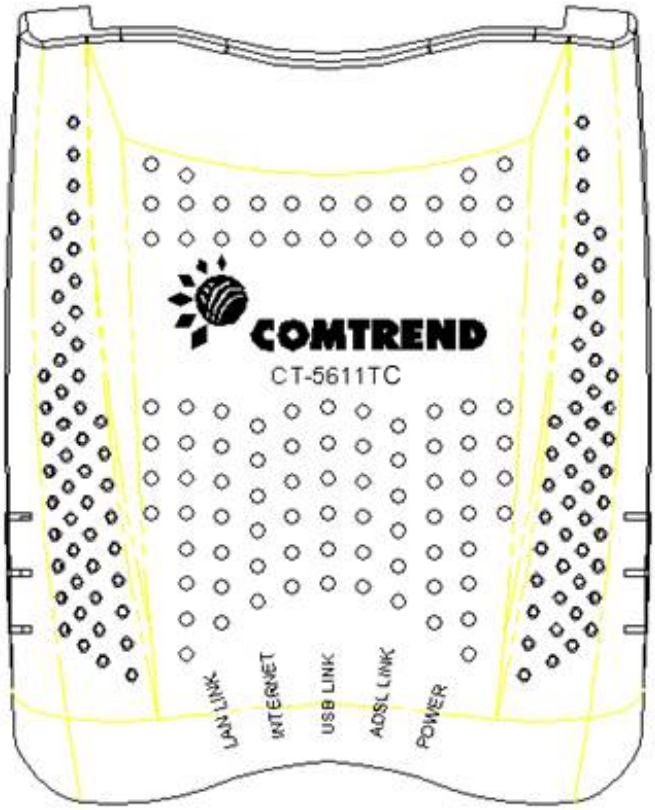
Power ON
Press the power button to the OFF position (OUT). Connect the power adapter to the power port. Attach the power adapter to a wall outlet or other AC source. Press the power button to the ON position (IN). If the Power LED indicator lights up (GREEN) then the device is ready for setup.

Caution 1:	If the device fails to power up, or it malfunctions, first verify that the power cords are connected securely. Then power it on again. If the problem persists, contact technical support.
Caution 2:	Before servicing or disassembling this equipment always disconnect all power cords and telephone lines from their outlets.

Reset Button
Restore the default parameters of the device by holding down the Reset button until the front panel LED indicators start blinking simultaneously (5 seconds). After the device has rebooted successfully, and if the connection is established, the LAN, ADSL or USB LEDs will light up, depending on the connection type.

2.2 Front Panel

The LED indicators labeled in this top-down view are explained in the table below. Use them to check the status of the device and its connections.



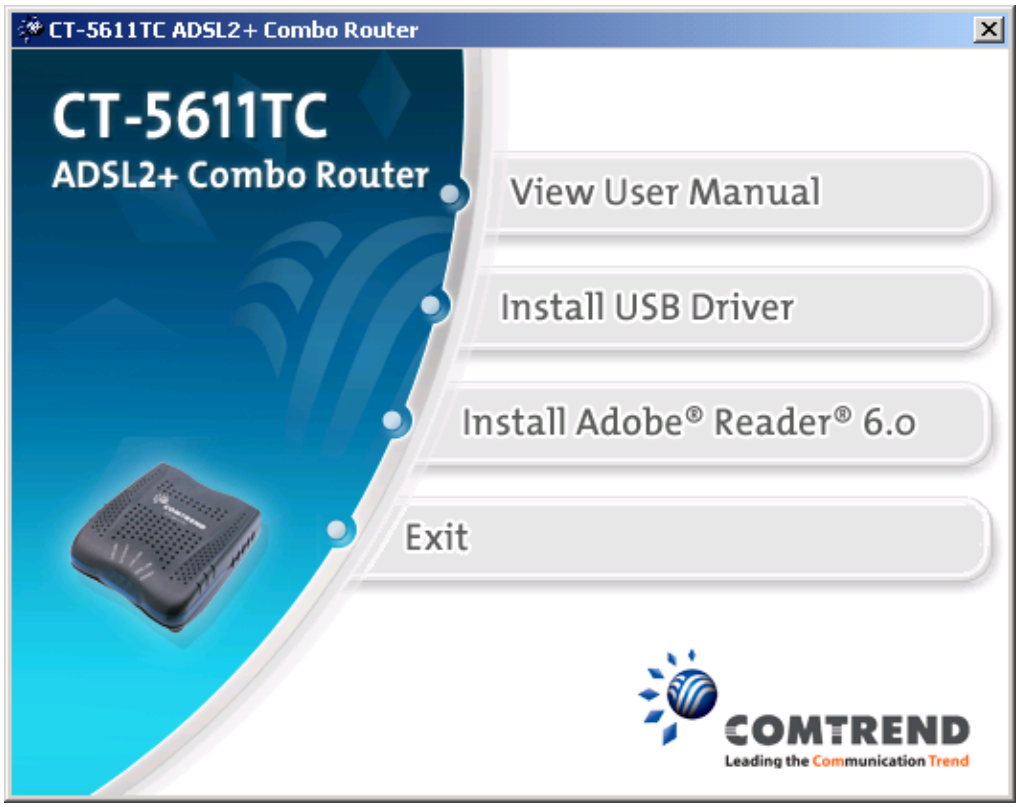
LED	Color	Mode	Function
LAN LINK	Green	On	An Ethernet Link is established.
		Off	An Ethernet Link is not established.
		Blink	Data transmitting or receiving over LAN.
INTERNET	Green	On	The INTERNET link is established.
		Off	The INTERNET link is not established.
		Blink	INTERNET link transmitting or receiving.
	Red	On	Device attempted to become IP connected and failed (no DHCP response, no PPPoE response, PPPoE authentication failed, no IP address from IPCP, etc.)
USB LINK	Green	On	A USB link is established.
		Off	A USB link is not established.
		Blink	Data transmitting or receiving over USB.
ADSL LINK	Green	On	The ADSL link is established.
		Off	The ADSL link is not established.
		Blink	The ADSL link is training.
POWER	Green	On	The device is powered up.
		Off	The device is powered down.
	Red	On	POST (Power On Self Test) failure or other malfunction. A malfunction is any error of internal sequence or state that will prevent the device from connecting to the DSLAM or passing customer data.

2.3 USB Driver Autorun Installation

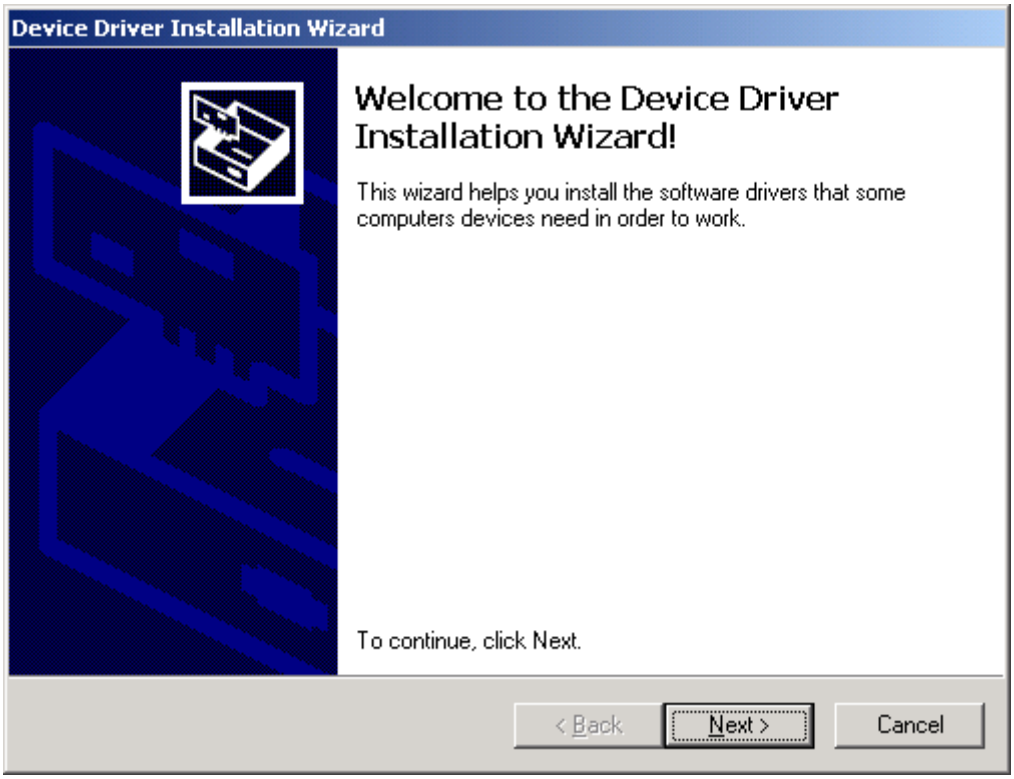
Before connecting the CT-5611TC to a PC with USB, the correct drivers must be installed. The auto-run USB driver installation supports Win ME, Win 98, Win 2000, Win XP (32 bit) and Vista (32 bit). For those using Windows XP 64 bit, the driver must be installed manually (please see section 2.3 below for details).

Follow the procedure below to install the standard (32 bit) USB driver

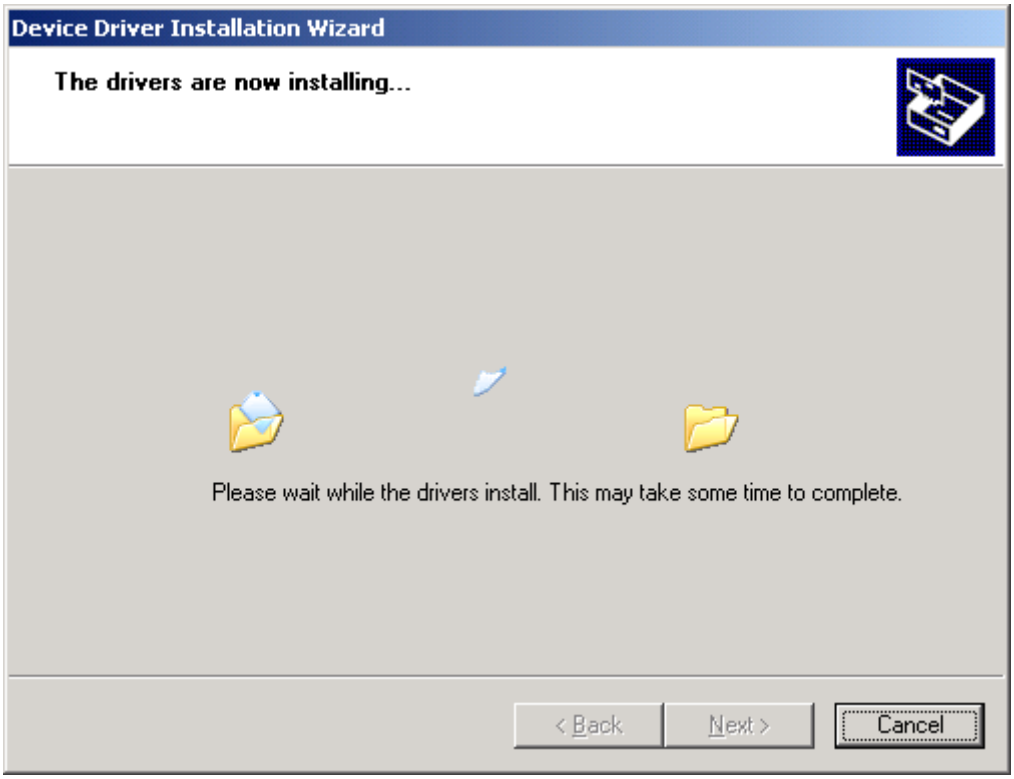
STEP 1: Insert the Installation CD and select **Install USB Driver** from the autostart menu shown below.



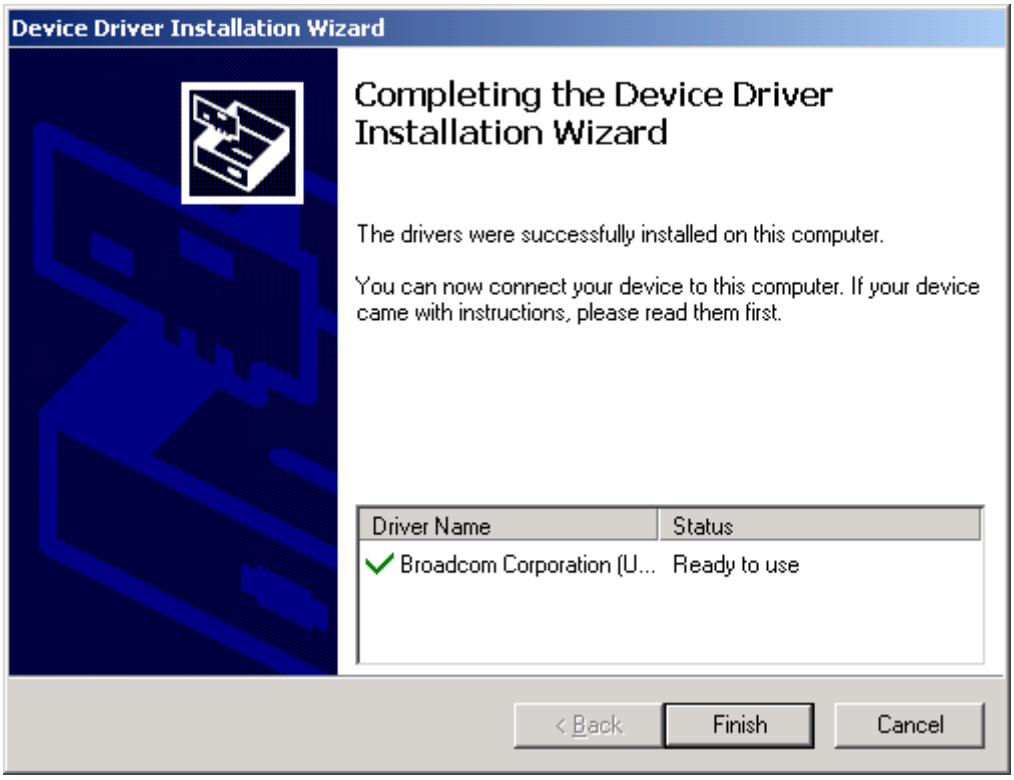
STEP 2: The following window will be displayed. Click the **Next** button to continue.


Device Driver Installation Wizard
Welcome to the Device Driver Installation Wizard!
This wizard helps you install the software drivers that some computers devices need in order to work.
To continue, click Next.
< Back
Next >
Cancel

STEP 3: When the window displays as below, wait for the drivers to fully install.


Device Driver Installation Wizard
The drivers are now installing...
Please wait while the drivers install. This may take some time to complete.
< Back
Next >
Cancel

STEP 4: Click the **Finish** button, when the window displays as below.


Device Driver Installation Wizard
Completing the Device Driver Installation Wizard
The drivers were successfully installed on this computer.
You can now connect your device to this computer. If your device came with instructions, please read them first.
Driver Name
Status
Broadcom Corporation (U...
Ready to use
< Back
Finish
Cancel

STEP 5: The installation is complete. You can now connect the device to your PC using a standard USB cable.

2.4 USB Driver Manual Installation (64bit OS)

Before connecting this router to a PC with USB, the correct drivers must be installed.

Follow the procedure below to manually install the 64bit USB driver

STEP 1: Connect the USB port to the PC by plugging the flat connector of a standard USB cable into your PC and plugging the square connector into the device. After a moment, the connection should be detected by your PC and if so the screen will display a notice to that effect, as shown below:

STEP 2: When the window displays as below, select **Install from a list or specific location (Advanced)** and then click the **Next** button.

Found New Hardware Wizard
Welcome to the Found New Hardware Wizard
This wizard helps you install software for:
USB Network Interface
If your hardware came with an installation CD or floppy disk, insert it now.
What do you want the wizard to do?
Install the software automatically (Recommended)
Install from a list or specific location (Advanced)
Click Next to continue.
< Back
Next >
Cancel

NOTE:	This window won't display if the USB Driver has been previously installed. In this case, contact technical support for assistance.

STEP 3: Insert the installation CD.

NOTE: If you see the autostart menu (as shown in **step 1** of previous section)

CLICK -

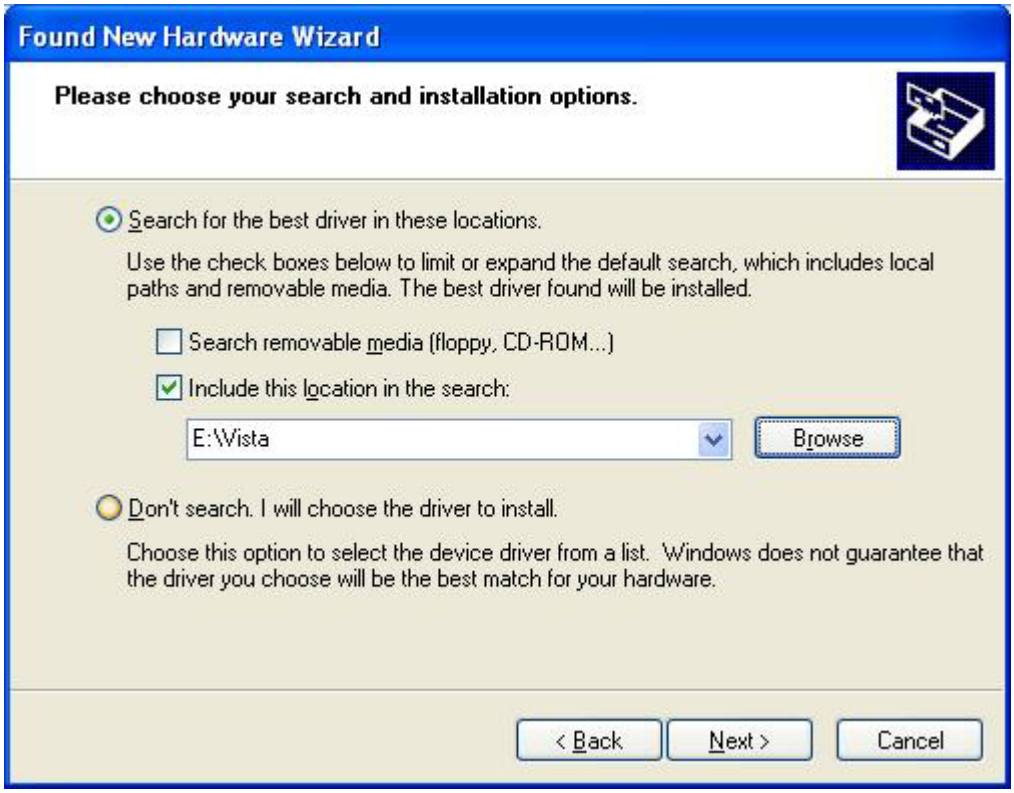
and continue with the manual installation process.

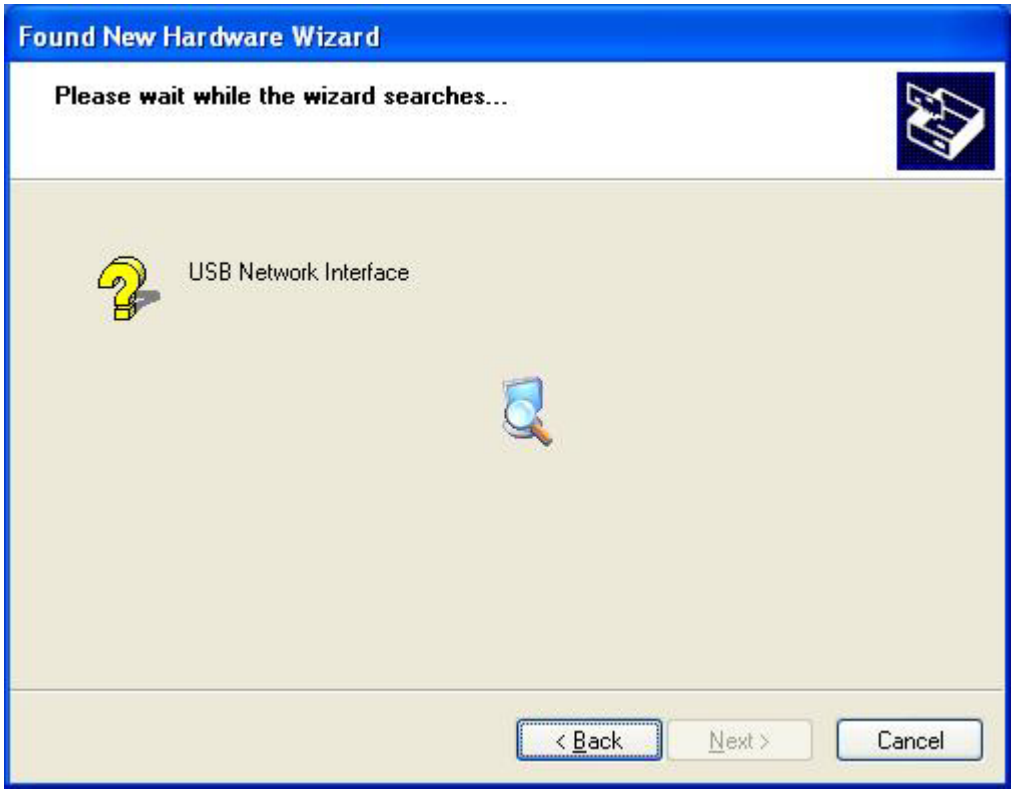
Found New Hardware Wizard
Please choose your search and installation options.
Search for the best driver in these locations.
Use the check boxes below to limit or expand the default search, which includes local paths and removable media. The best driver found will be installed.
Search removable media (floppy, CD-ROM...)
Include this location in the search:
Browse
Don't search. I will choose the driver to install.
Choose this option to select the device driver from a list. Windows does not guarantee that the driver you choose will be the best match for your hardware.
< Back
Next >
Cancel

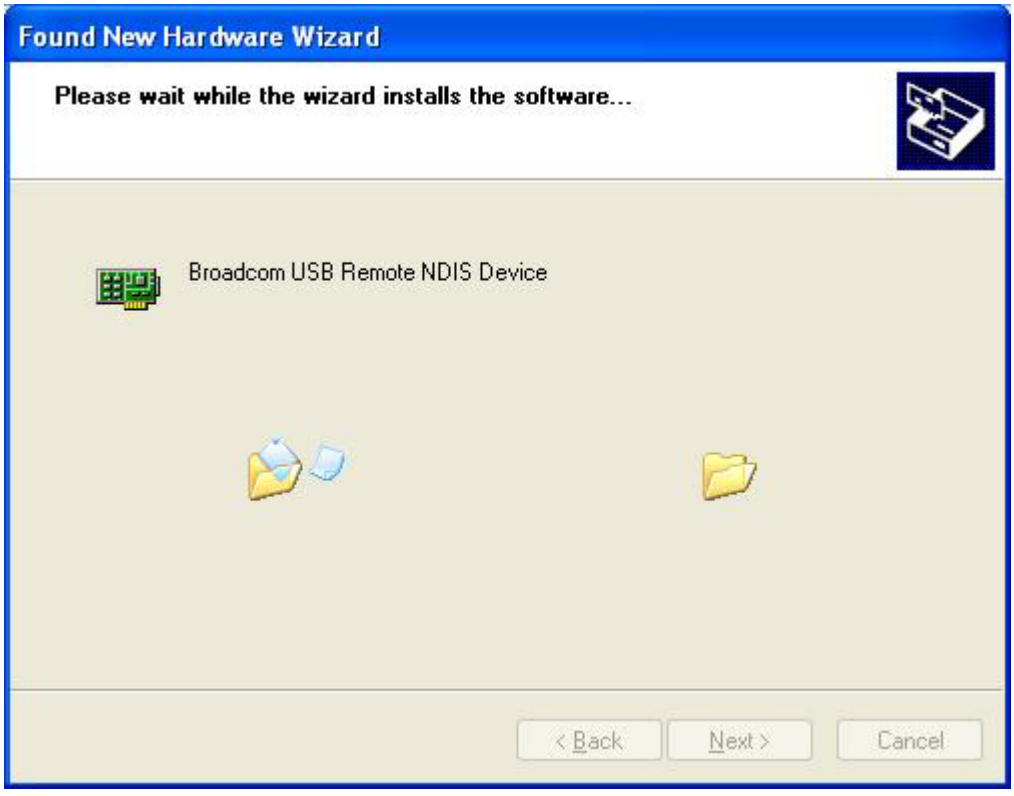
STEP 4: Select the location of the file using the **Browse** button, as shown above. Normally, the file is on the CD-ROM shipped with the device.

STEP 5: Locate the **Vista** folder, and click **OK**.

STEP 6: When the window displays as below, click **Next** and then wait.


Found New Hardware Wizard
Please choose your search and installation options.
Search for the best driver in these locations.
Use the check boxes below to limit or expand the default search, which includes local paths and removable media. The best driver found will be installed.
Search removable media (floppy, CD-ROM...)
Include this location in the search:
E:\Vista
Browse
Don't search. I will choose the driver to install.
Choose this option to select the device driver from a list. Windows does not guarantee that the driver you choose will be the best match for your hardware.
< Back
Next >
Cancel





STEP 7: Click the **Finish** button when the window displays as below.

Found New Hardware Wizard
Completing the Found New Hardware Wizard
The wizard has finished installing the software for:
Broadcom USB Remote NDIS Device
Click Finish to close the wizard.
< Back
Finish
Cancel

STEP 8: Installation is complete. You can now use the USB connection.

Chapter 3 Web User Interface

This section describes how to access the device via the web user interface (WUI) using an Internet browser such as Internet Explorer (version 5.0 and later).

3.1 Default Settings

The following are the default settings for the device:

- LAN IP address: 192.168.1.1 / Subnet mask: 255.255.255.0
- Administrative access (username: **root** , password: **12345**)
- User access (username: **user**, password: **user**)

- DHCP server: **enabled** in routing modes (PPPoA/E, IPoA & MER)

- Firewall and NAT: **enabled** for PPPoE and PPPoA
  disabled for Bridge*, MER and IPoA
  (* NAT is not available in Bridge mode)

- WAN IP address: none
- Remote WAN access: **disabled**
- Remote (WAN) access (username: **support**, password: **support**)

This device supports the following connection types.

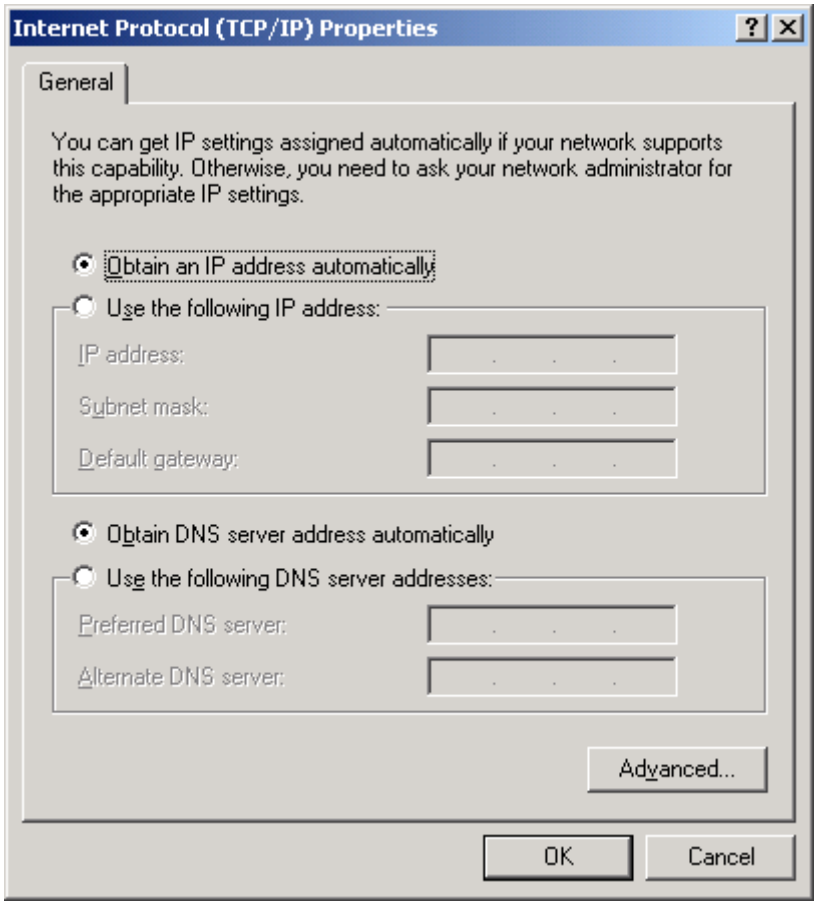
- PPP over Ethernet (PPPoE)
- PPP over ATM (PPPoA)
- MAC Encapsulated Routing (MER)
- IP over ATM (IPoA)
- Bridging

Technical Note:
During power on, the device initializes all settings to default values. It will then read the configuration profile from the permanent storage section of flash memory. The default attributes are overwritten when identical attributes with different values are configured. The configuration profile in permanent storage can be created via the web user interface or telnet user interface, or other management protocols. The factory default configuration can be restored either by pushing the reset button for more than five seconds until the power indicates LED blinking or by clicking the Restore Default Configuration option in the Restore Settings screen.

3.2 IP Configuration

DHCP Mode

When the device powers up, the DHCP server (on the device) will start automatically. To set your PC for DHCP mode, check the Internet Protocol properties of your Local Area Connection. You can set your PC to DHCP mode by selecting **Obtain an IP address automatically** in the dialog box shown below.

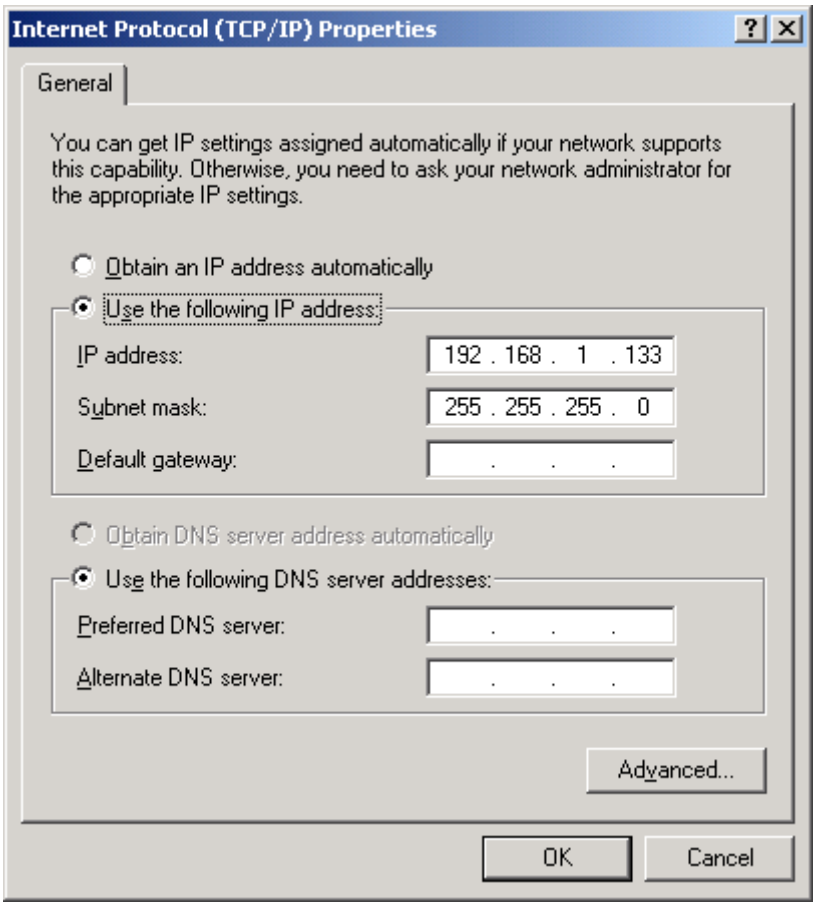

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

STATIC IP Mode

To configure the device manually, your PC must have a static IP address within the 192.168.1.x subnet. Follow the steps below to configure your PC IP address to use subnet 192.168.1.x. The following assumes you are running Windows XP.

STEP 1: From the Network Connections window, open Local Area Connection (*You may also access this screen by double-clicking the Local Area Connection icon on your taskbar*). Click the **Properties** button.

STEP 2: **Select Internet Protocol (TCP/IP)** and click the **Properties** button. The screen should now display as below. Change the IP address to the domain of 192.168.1.x (1<x<254) with subnet mask of 255.255.255.0.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 1 . 133
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

STEP 3: Click **OK** to submit the settings.

3.3 Login Procedure

Perform the following steps to login to the web user interface.

NOTE:	The default settings can be found in 3.1 Default Settings.

STEP 1: Start the Internet browser and enter the default IP address for the device in the Web address field. For example, if the default IP address is 192.168.1.1, type http://192.168.1.1.

NOTE:	For local administration (i.e. LAN access), the PC running the browser must be attached to the Ethernet, and not necessarily to the device. For remote access (i.e. WAN), use the IP address shown on the Device Info - WAN screen and login with remote username and password.

STEP 2: A dialog box will appear, such as the one below. Enter a default username and password, as defined in section 3.1 Default Settings.

Click **OK** to continue.

NOTE:	The login password can be changed later (see 8.6.3 Passwords)

STEP 3: After successfully logging in for the first time, you will reach this screen.

NOTE1:	If a PVC connection already exists then this Quick Setup screen will be bypassed and the Device Info – Summary screen will display instead.
NOTE2:	The selections available on the main menu (onscreen at left) are based upon the configured connection and user account privileges.

Chapter 4 Quick Setup

The function allows the user to configure the ADSL router for DSL connectivity and Internet access. It guides the user though the WAN network setup first and then the LAN interface setup. The user can either manually customize the router or follow the auto quick setup procedure.

The following configuration considerations apply:

- The WAN network operating mode operation depends on the service provider's configuration on the Central Office side and Broadband Access Server for the PVC
- If the service provider provides PPPoE service, then the connection selection depends on whether the LAN-side device (typically a PC) is running a PPPoE client or whether the CT-5611TC is to run the PPPoE client. The CT-5611TC can support both cases simultaneously.
- If some or none of the LAN-side devices are not running a PPPoE client, then select PPPoE. If all LAN-side devices are running PPPoE clients, then select Bridge In PPPoE mode, CT-5611TC also supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client from non-PPPoE LAN devices.
- NAT and firewall are always enabled when PPPoE mode is selected, but they can be enabled or disabled by the user when MER or IPoA is selected, NAT and firewall are always disabled when Bridge mode is selected.
- Depending on the network operating mode, and whether NAT and firewall are enabled or disabled, the main menu will display or hide the NAT/Firewall menu. For instance, if the default network operating mode is Bridge, the main menu will not show the NAT and Firewall menu.

NOTE:	Up to eight PVC profiles can be configured and saved on the flash memory. To activate a particular PVC profile, you need to navigate through all the Quick Setup screens until the last summary screen, then click the **Save/Reboot** button to apply settings and reboot the device.

4.1 Auto Quick Setup

The auto quick setup procedures requires the ADSL link to be up to automatically detect PVCs. You simply need to follow the online instructions as prompted.

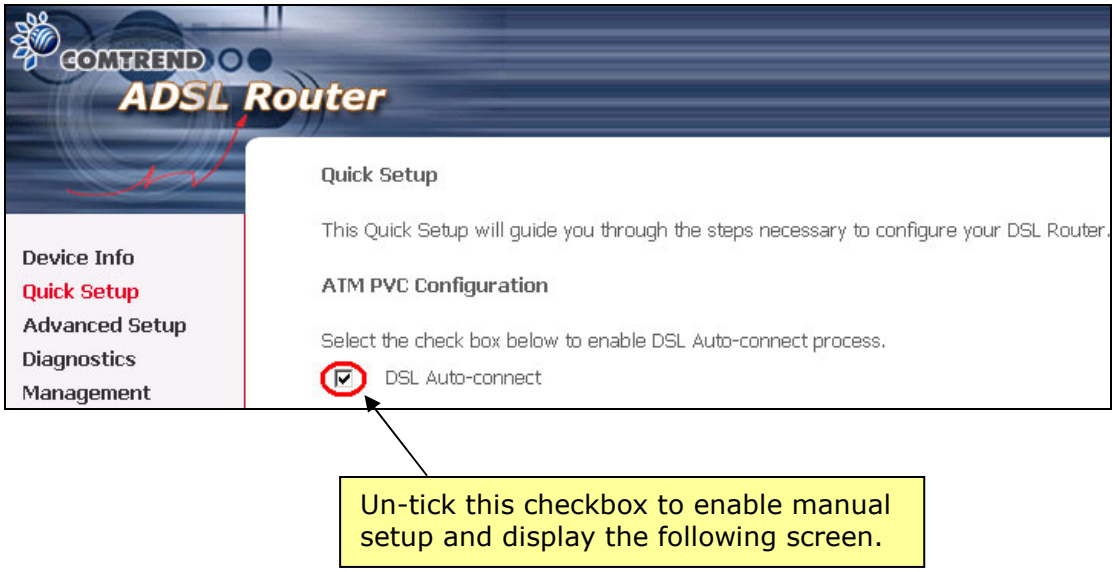
Step 1: Select Quick Setup to display the DSL Quick Setup screen.

Step 2: Click **Next** to start the setup process. Follow the online instructions to complete the setting. This procedure will skip some advanced setup procedures (such as PVC index and encapsulation selection).

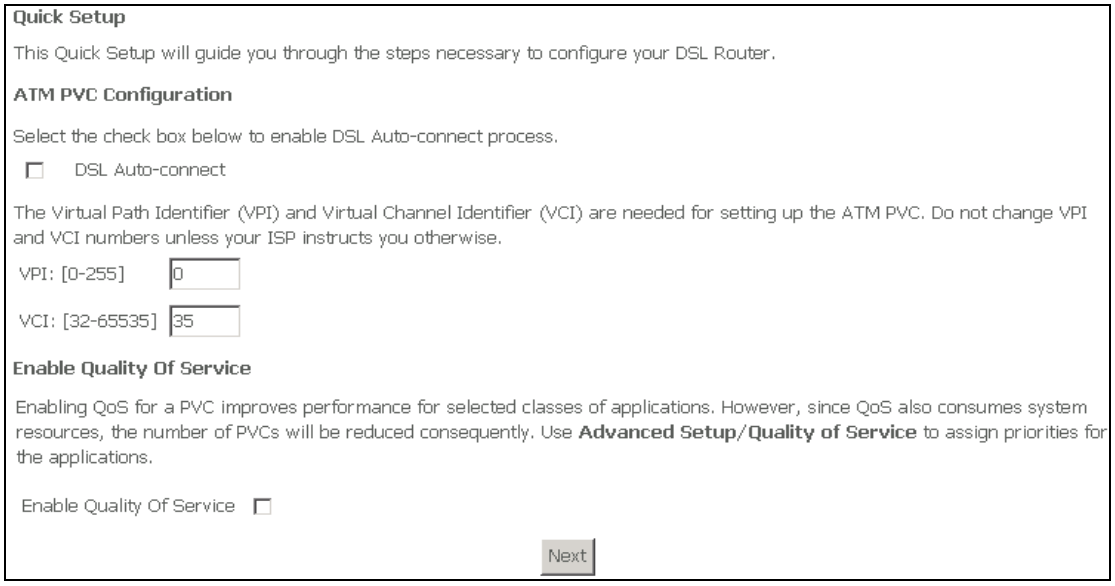
Step 3: After the settings are complete, you can use the ADSL service.

4.2 Manual Quick Setup

STEP 1: Click Quick Setup and un-tick the DSL Auto-connect checkbox to enable manual configuration of the connection type.

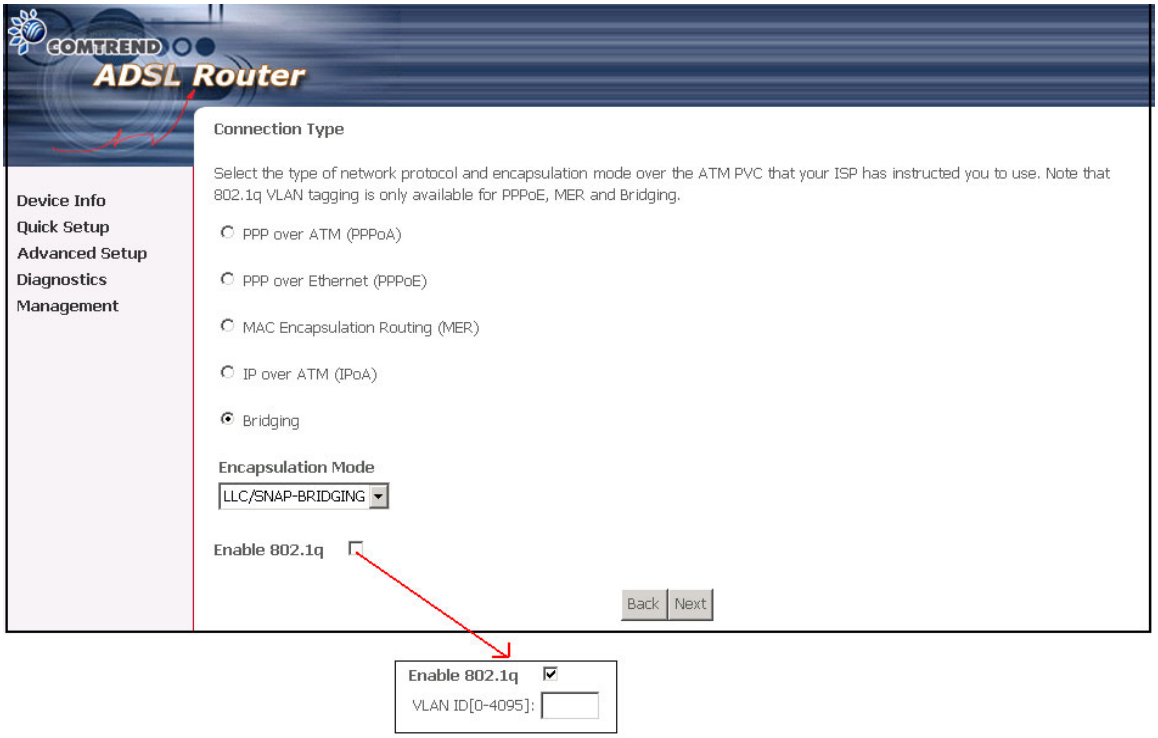


Un-tick this checkbox to enable manual setup and display the following screen.


Quick Setup
This Quick Setup will guide you through the steps necessary to configure your DSL Router.
ATM PVC Configuration
Select the check box below to enable DSL Auto-connect process.
DSL Auto-connect
The Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) are needed for setting up the ATM PVC. Do not change VPI and VCI numbers unless your ISP instructs you otherwise.
VPI: [0-255] 0
VCI: [32-65535] 35
Enable Quality Of Service
Enabling QoS for a PVC improves performance for selected classes of applications. However, since QoS also consumes system resources, the number of PVCs will be reduced consequently. Use Advanced Setup/Quality of Service to assign priorities for the applications.
Enable Quality Of Service
Next

STEP 2: Enter the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI). Select Enable Quality Of Service if required. Click **Next**.

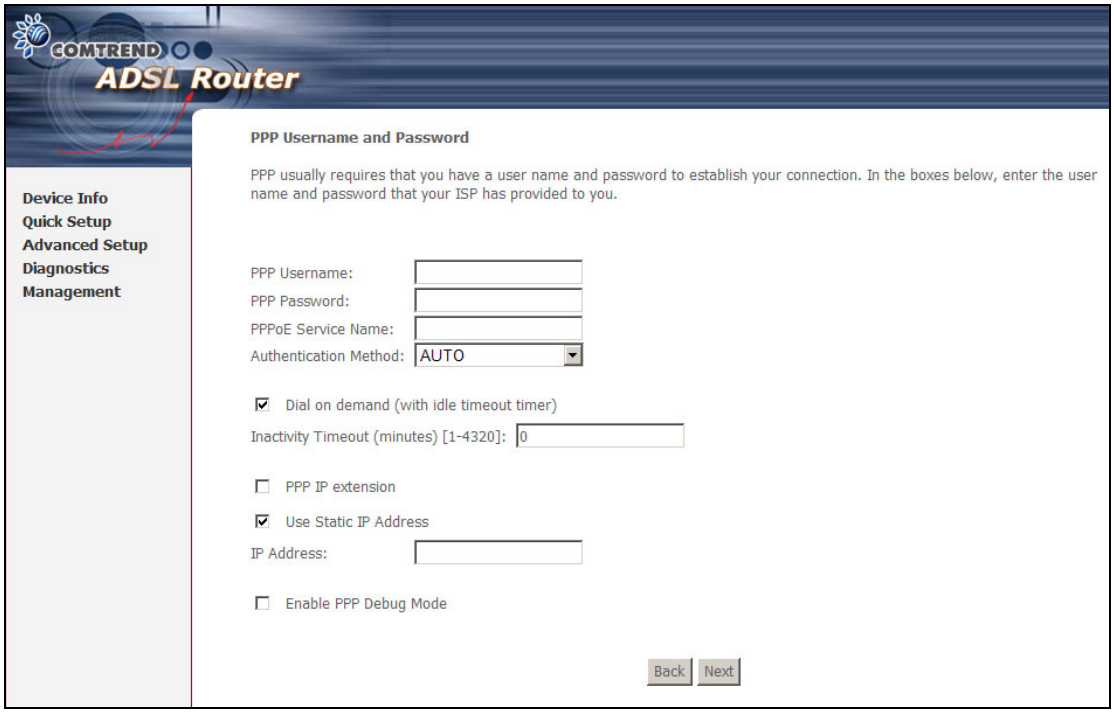
STEP 3: Choose the connection type and encapsulation mode.



STEP 4: Choosing different connection types pops up different encapsulation. Enter appropriate settings as requested by your service provider. The following descriptions state each connection type setup separately. Select **Enable 802.1q** (by ticking the box) if required, and input a number for the VLAN ID. Click on **Next** to go to next step.

4.2.1 PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE)

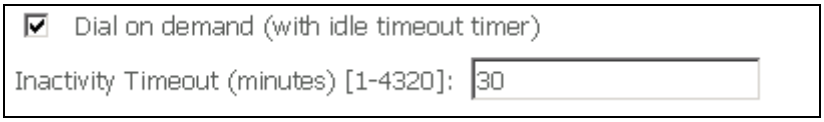
Step 1: Select the **PPP over ATM (PPPoA)** or **PPP over Ethernet (PPPoE)** radio button and click **Next**. The following screen appears:



PPP Username/PPP Password
The PPP Username and the PPP password requirement are dependent on the particular requirements of the ISP or the ADSL service provider. The WEB user interface allows a maximum of 256 characters in the PPP user name and a maximum of 32 characters in PPP password.

Authentication Method
Choose from AUTO, PAP, CHAP and MSCHAP.

Dial on Demand
The CT-5611TC can be configured to disconnect if there is no activity for a period of time by selecting the Dial on demand check box. When the checkbox is ticked, you need to enter the inactivity timeout period. The timeout period ranges from 1 minute to 4320 minutes.



PPP IP Extension
The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider specially requires this setup, do not select it.
The PPP IP Extension supports the following conditions:

- Allows only one PC on the LAN
- The public IP address assigned by the remote side using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC's LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the ADSL router has a single IP address to assign to a LAN device.
- NAPT and firewall are disabled when this option is selected.
- The ADSL router becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The ADSL router extends the IP subnet at the remote service provider to the

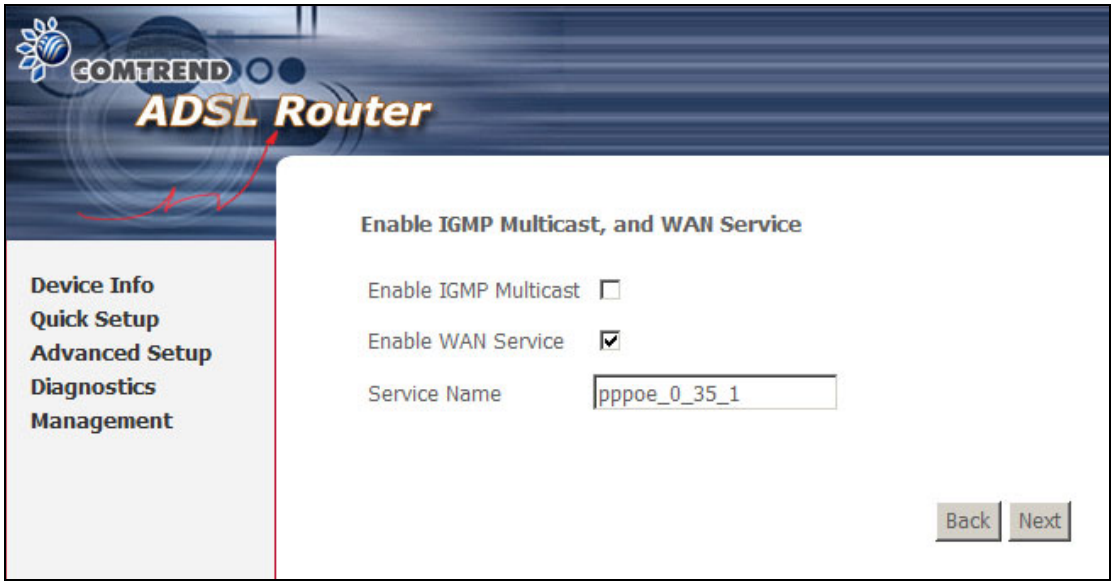
LAN PC. That is, the PC becomes a host belonging to the same IP subnet.

- The ADSL router bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the router's LAN IP address.

Use Static IP Address
Unless your service provider specially requires this setup, do not select it.
If selected, enter your static IP address.

Enable PPP Debug Mode
Tick the checkbox to enable this function.

Step 2: Click **Next** to display the screen below.



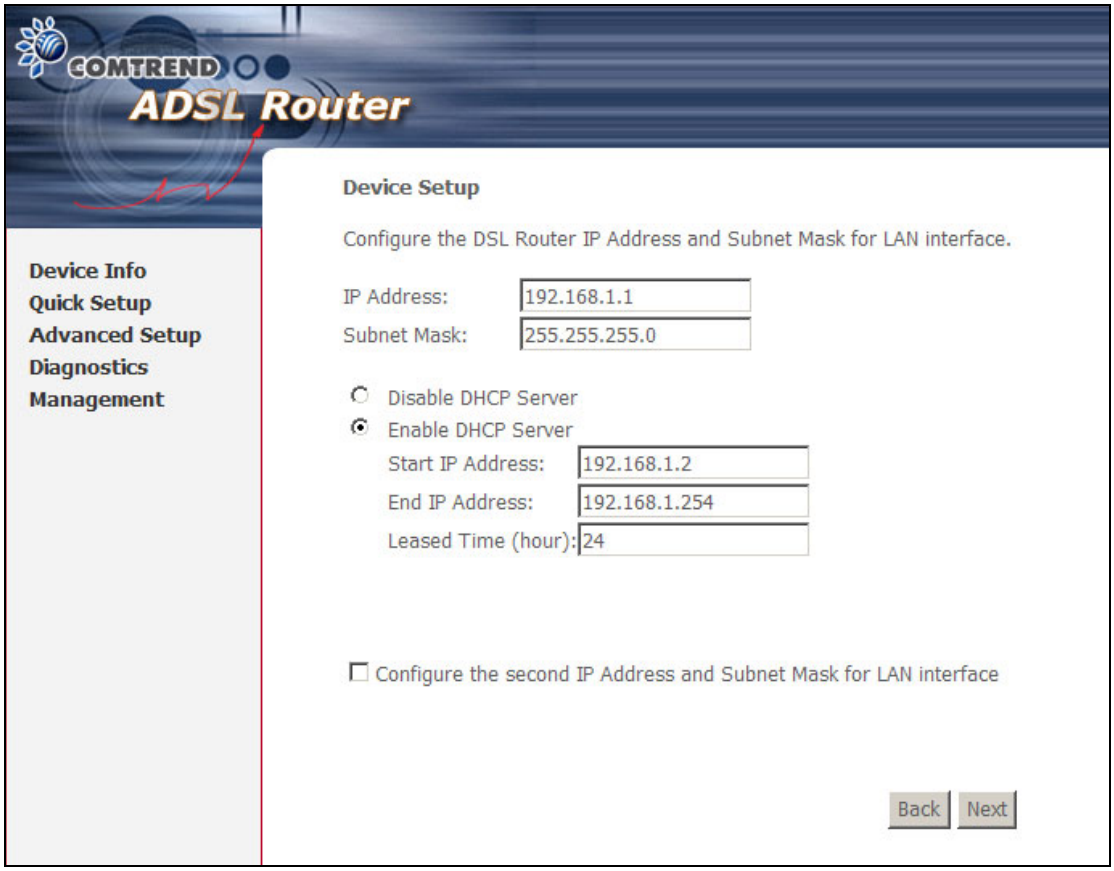
Enable IGMP Multicast checkbox: Tick the checkbox to enable IGMP multicast (proxy). IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers.

Enable WAN Service checkbox: Tick this item to enable the ATM service. Untick it to stop the ATM service.

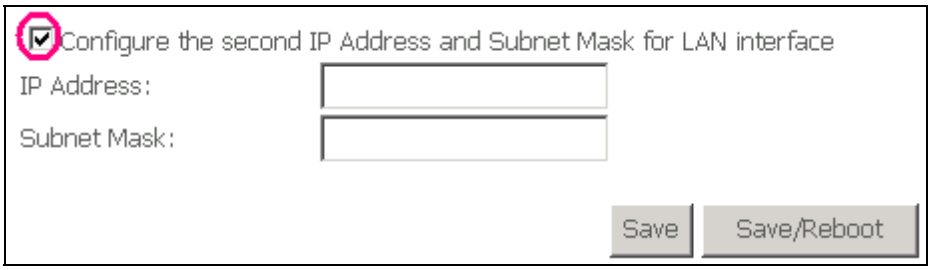
Service Name: This is user-defined.

Step 3: After entering your settings, click **Next**. The following screen appears.

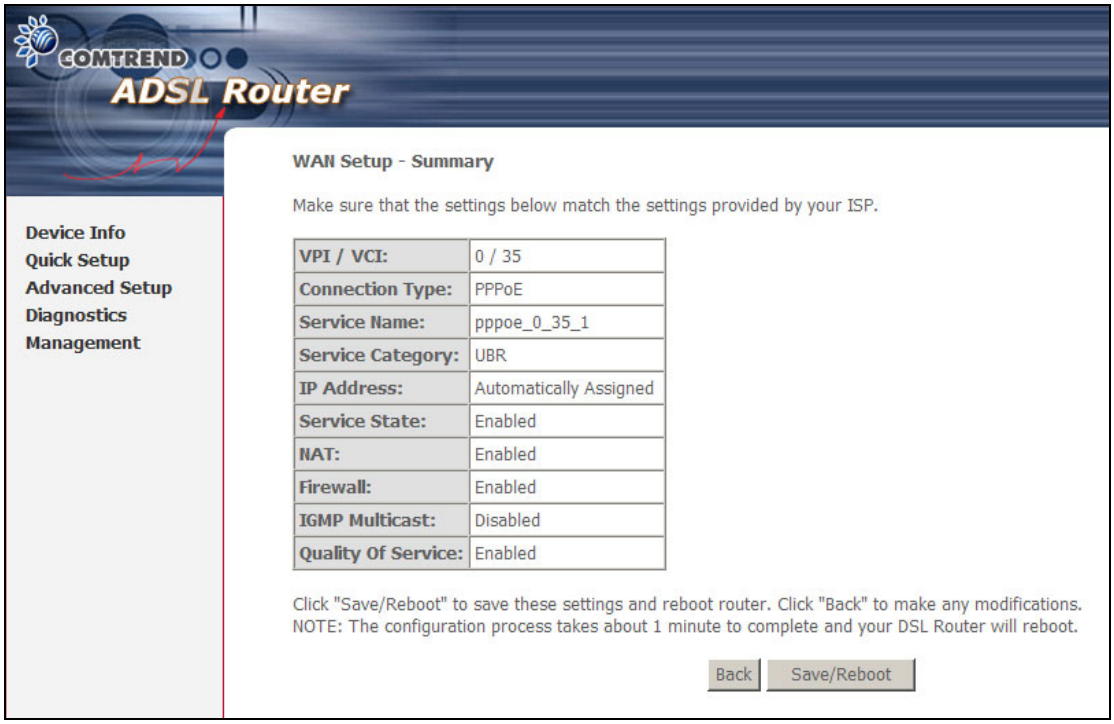
The Device Setup screen allows the user to configure the LAN interface IP address, subnet mask and DHCP server. If the user would like this ADSL router to assign dynamic IP addresses, DNS server and default gateway to other LAN devices, select the radio box **Enable DHCP server** and enter the Start/End IP addresses and DHCP lease time. This configures the router to automatically assign IP addresses, default gateway address and DNS server addresses to each of your PCs.



To configure a secondary IP address for the LAN port, click the checkbox below.



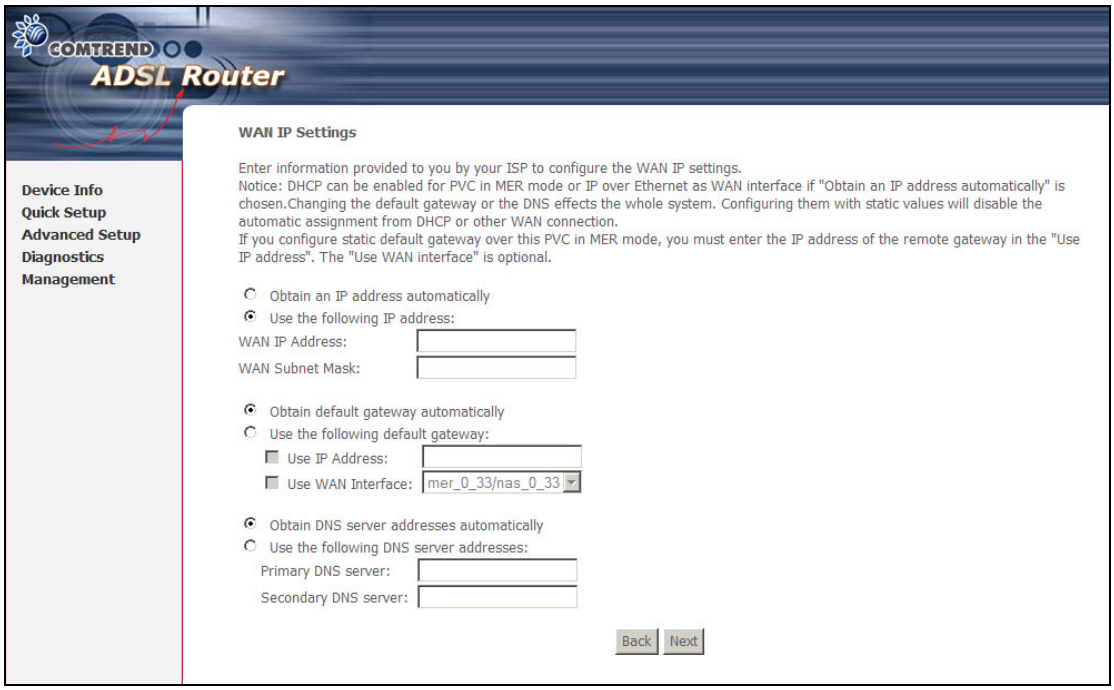
Step 4: Click **Next** to display the WAN Setup-Summary screen that presents the entire configuration summary. Click **Save/Reboot** if the settings are correct. Click **Back** if you wish to modify the settings.


COMTREND
ADSL Router
Device Info
Quick Setup
Advanced Setup
Diagnostics
Management
WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
VPI / VCI: 0 / 35
Connection Type: PPPoE
Service Name: pppoe_0_35_1
Service Category: UBR
IP Address: Automatically Assigned
Service State: Enabled
NAT: Enabled
Firewall: Enabled
IGMP Multicast: Disabled
Quality Of Service: Enabled
Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.
Back
Save/Reboot

Step 5: After clicking **Save/Reboot**, the router will save the configuration to the flash memory and then reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Device Info screen automatically. The CT-5611TC is ready for operation and the LEDs display as described in the LED description tables.

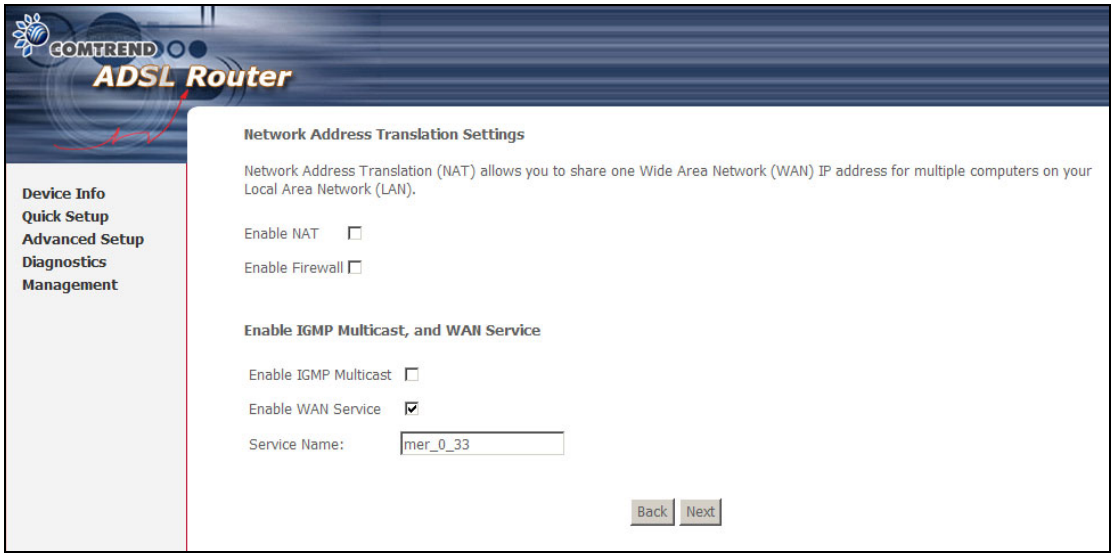
4.2.2 MAC Encapsulation Routing (MER)

Step 1: Enter the WAN IP settings as directed by your ISP.


COMTREND
ADSL Router
Device Info
Quick Setup
Advanced Setup
Diagnostics
Management
WAN IP Settings
Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: DHCP can be enabled for PVC in MER mode or IP over Ethernet as WAN interface if "Obtain an IP address automatically" is chosen.Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection.
If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address". The "Use WAN interface" is optional.
Obtain an IP address automatically
Use the following IP address:
WAN IP Address:
WAN Subnet Mask:
Obtain default gateway automatically
Use the following default gateway:
Use IP Address:
Use WAN Interface: mer_0_33/nas_0_33
Obtain DNS server addresses automatically
Use the following DNS server addresses:
Primary DNS server:
Secondary DNS server:
Back
Next

NOTE: The DHCP Client can be enabled for PVC in MER mode if **Obtain an IP address automatically** is chosen. Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection. If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the **Use IP address** field.

Step 2: Click **Next** to display the following screen.



Enable NAT checkbox: If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu will be displayed on the advanced setup menu after reboot. The user can then configure NAT-related features after the system comes up. If a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox should be de-selected. When the system comes back after reboot, the NAT submenu will not be displayed on the left main menu. The default setting for MER is disabled.

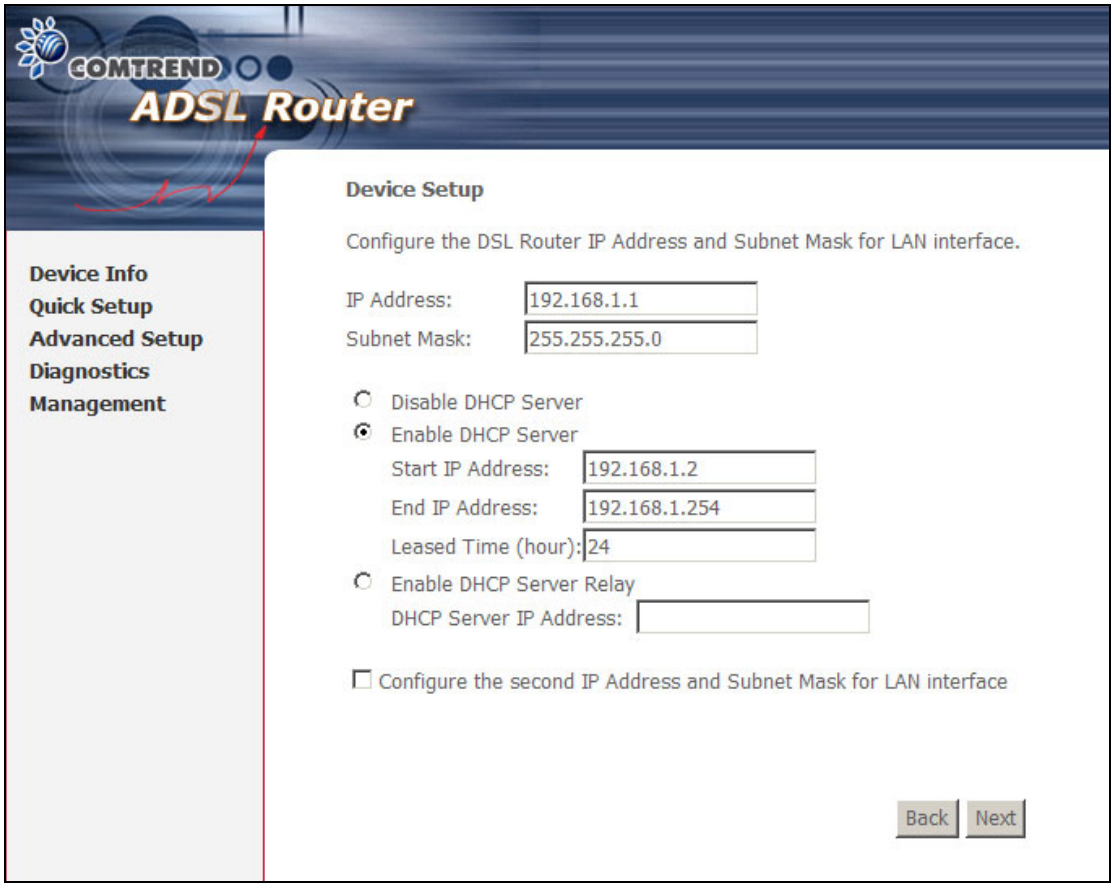
Enable Firewall checkbox: If the firewall checkbox is selected, the security submenu will be displayed on the advanced setup menu after reboot. The user can then configure firewall features after the system comes up. If firewall is not used, this checkbox should be de-selected to free up system resources for better performance. When system comes back after reboot, the Security submenu will not be displayed on the left main menu. The default setting for MER is disabled.

Enable IGMP Multicast: Tick the checkbox to enable IGMP multicast (proxy). IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers.

Enable WAN Service: Tick the checkbox to enable the WAN (ADSL) service. If this item is not selected, you will not be able to use the ADSL service.

Service Name: This is User-defined.

Step 3: Upon completion click **Next**. The following screen appears.

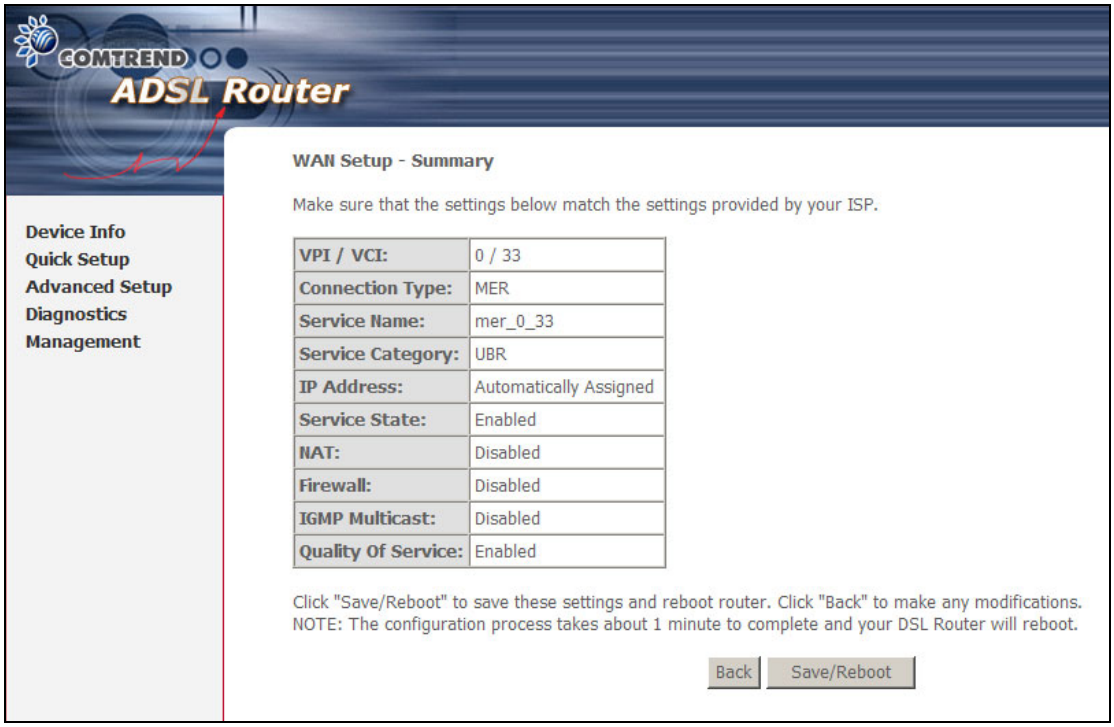


The Device Setup screen allows the user to configure the LAN interface IP address and DHCP server. If the user would like this ADSL router to assign dynamic IP addresses, DNS server and default gateway to other LAN devices, select the radio box **Enable DHCP server on the LAN** to enter the starting IP address and end IP address and DHCP lease time. This configures the router to automatically assign IP addresses, default gateway address and DNS server addresses to each of your PCs. Select **Enable DHCP Server Relay** (if required), and enter the DHCP Server IP Address.

NOTE 1: Enable DHCP Server Relay will not display if NAT is enabled.

NOTE 2: Ethernet and USB interfaces share the same subnet since they are bridged within the router.

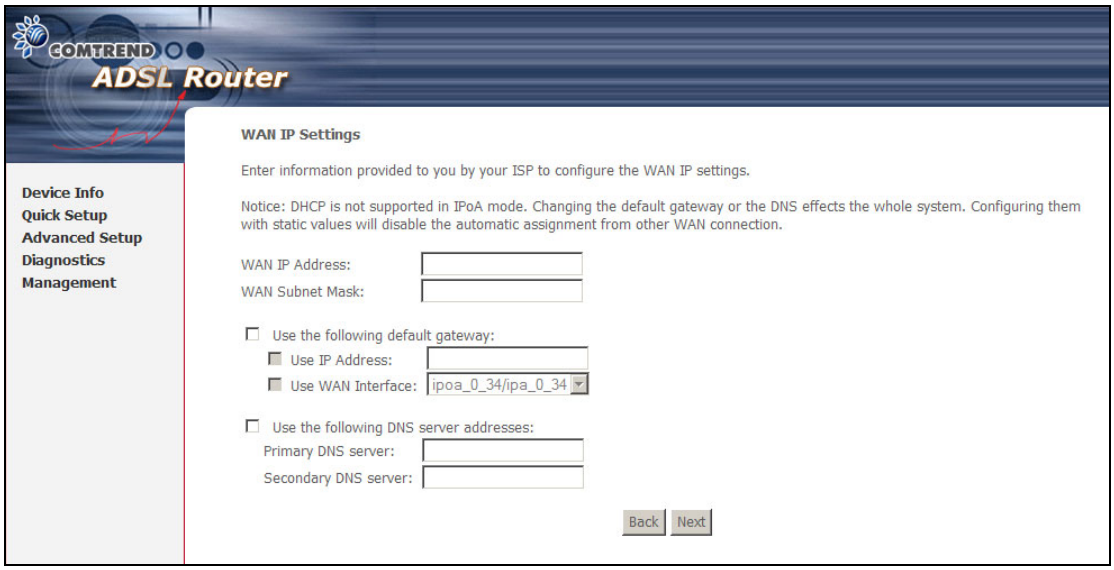
Step 4: After entering your settings, select **Next** to display the following screen. The WAN Setup-Summary screen presents the entire configuration summary. Click **Save/Reboot** if the settings are correct. Click **Back** if you wish to modify the settings.


COMTREND
ADSL Router
Device Info
Quick Setup
Advanced Setup
Diagnostics
Management
WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
VPI / VCI: 0 / 33
Connection Type: MER
Service Name: mer_0_33
Service Category: UBR
IP Address: Automatically Assigned
Service State: Enabled
NAT: Disabled
Firewall: Disabled
IGMP Multicast: Disabled
Quality Of Service: Enabled
Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.
Back
Save/Reboot

Step 5: After clicking **Save/Reboot**, the router will save the configuration to the flash memory, and reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Device Info screen automatically. The CT-5611TC is ready for operation and the LEDs display as described in the LED description tables.

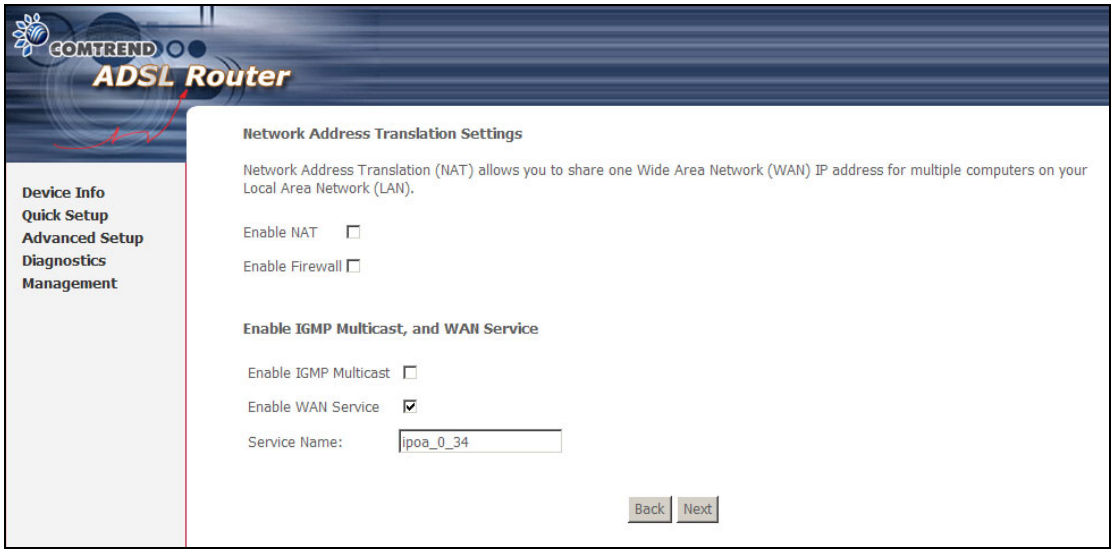
4.2.3 IP Over ATM

Step 1: Enter the WAN IP settings as directed by your ISP.


COMTREND
ADSL Router
Device Info
Quick Setup
Advanced Setup
Diagnostics
Management
WAN IP Settings
Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: DHCP is not supported in IPoA mode. Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from other WAN connection.
WAN IP Address:
WAN Subnet Mask:
Use the following default gateway:
Use IP Address:
Use WAN Interface: ipoa_0_34/ipa_0_34
Use the following DNS server addresses:
Primary DNS server:
Secondary DNS server:
Back
Next

NOTE: DHCP is not supported over IPoA. The user must enter the IP address or WAN interface for the default gateway setup and the DNS server addresses as directed by their ISP.

Step 2: Click **Next**. The following screen appears.



Enable NAT checkbox
If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu will be displayed on the advanced setup menu after reboot. The user can then configure NAT-related features after the system comes up. If a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox should be de-selected. When the system comes back after reboot, the NAT submenu will not be displayed on the left main menu. The default setting for MER is disabled.

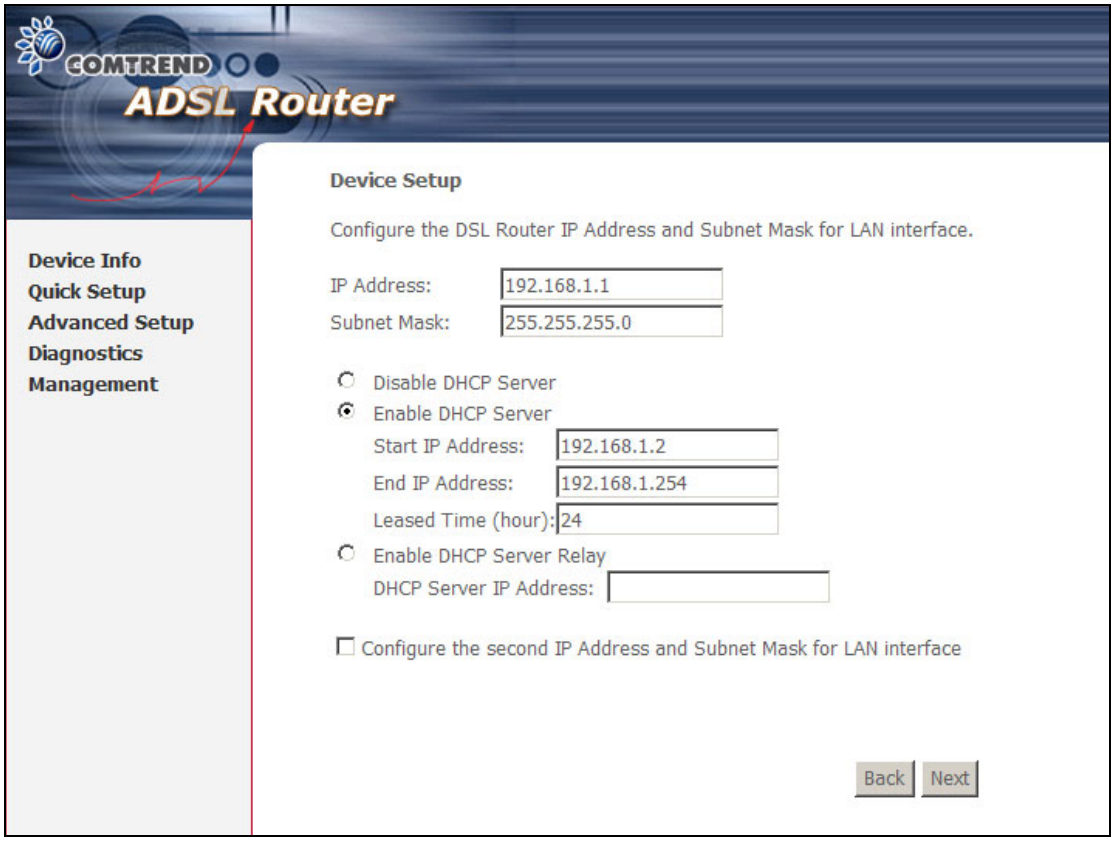
Enable Firewall checkbox
If the firewall checkbox is selected, the security submenu will be displayed on the advanced setup menu after reboot. The user can then configure firewall features after the system comes up. If firewall is not used, this checkbox should be de-selected to free up system resources for better performance. When system comes back after reboot, the Security submenu will not be displayed on the left main menu. The default setting for MER is disabled.

Enable IGMP Multicast: Tick the checkbox to enable IGMP multicast (proxy). IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers.

Enable WAN Service: Tick the checkbox to enable the WAN (ADSL) service. If this item is not selected, you will not be able to use the ADSL service.

Service Name: This is User-defined.

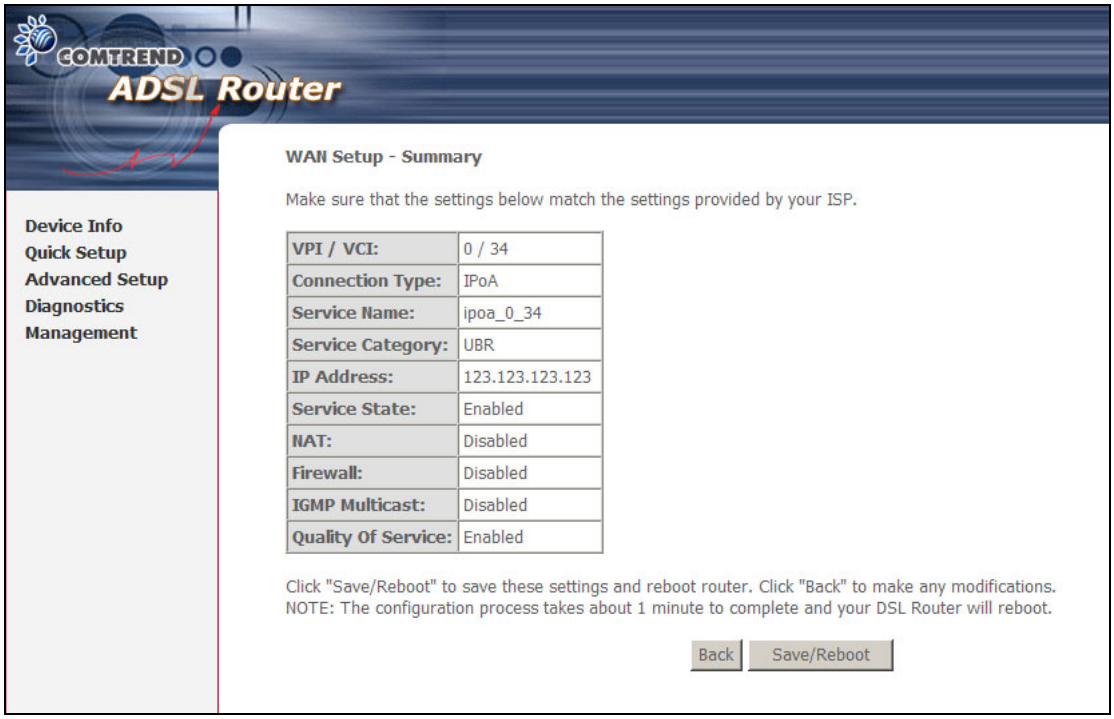
Step 3: Click **Next** to display the following screen. The Device Setup screen allows the user to configure the LAN interface IP address and subnet mask of the ADSL router. Select **Enable DHCP server** and enter Start/End IP address and DHCP lease time to assign dynamic IP addresses, DNS server and default gateway to other LAN devices.



NOTE : Enable DHCP Server Relay will not display if NAT is enabled.

The user must configure the IP Address and the Subnet Mask. To use the DHCP service on the LAN, select the **Enable DHCP server** checkbox, and enter the Start IP addresses, the End IP address and DHCP lease time. This configures the router to automatically assign IP addresses, default gateway address and DNS server addresses to each of your PCs. Select **Enable DHCP Server Relay** (if required), and enter the DHCP Server IP Address.

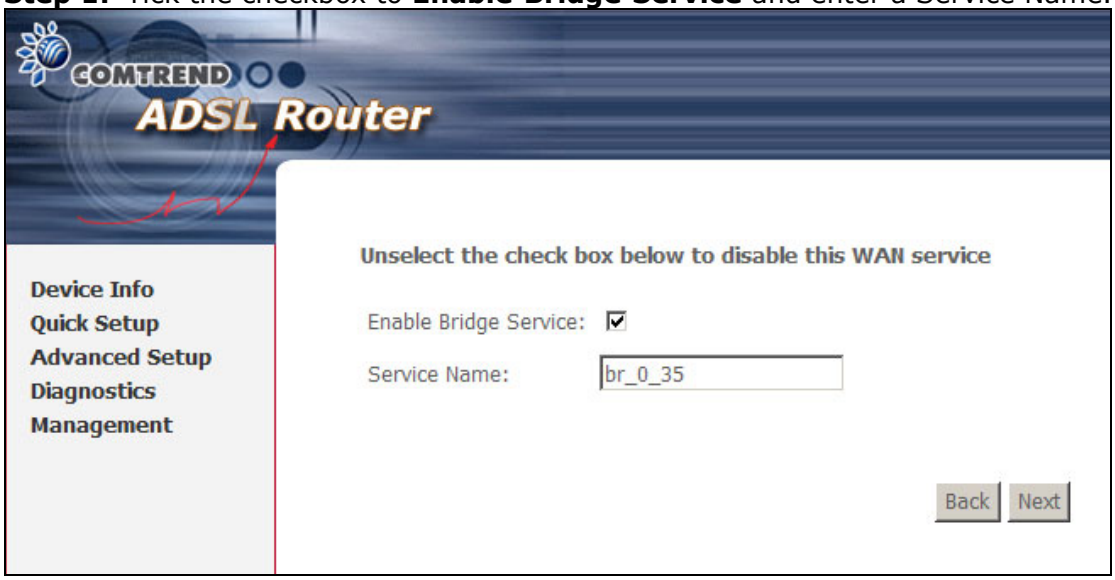
Step 4: The WAN Setup-Summary screen presents the entire configuration summary. Click **Save/Reboot** if the settings are correct. Click **Back** to modify the settings.


COMTREND
ADSL Router
Device Info
Quick Setup
Advanced Setup
Diagnostics
Management
WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
VPI / VCI: 0 / 34
Connection Type: IPoA
Service Name: ipoa_0_34
Service Category: UBR
IP Address: 123.123.123.123
Service State: Enabled
NAT: Disabled
Firewall: Disabled
IGMP Multicast: Disabled
Quality Of Service: Enabled
Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.
Back
Save/Reboot

Step 5: After clicking **Save/Reboot**, the router will save the configuration to the flash memory, and reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Device Info screen automatically. The CT-5611TC is ready for operation and the LEDs display as described in the LED description tables.

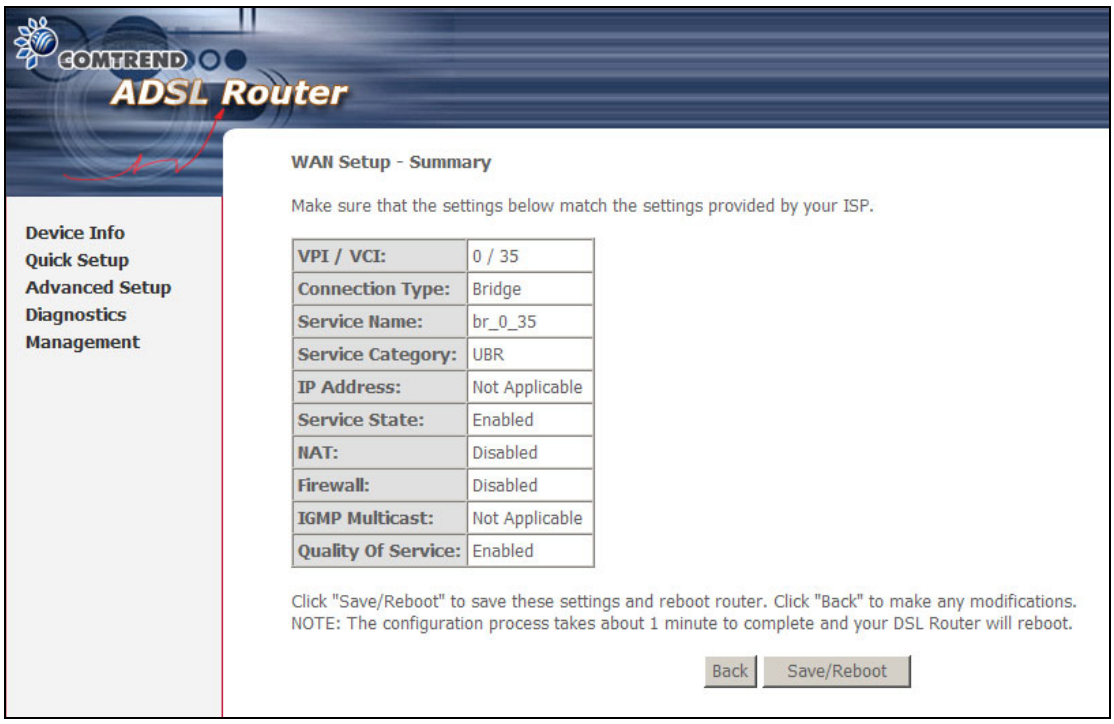
4.2.4 Bridging

Step 1: Tick the checkbox to **Enable Bridge Service** and enter a Service Name.



Step 2: Click the **Next** button to continue. Enter the IP address for the LAN interface. The LAN IP interface in bridge operating mode is needed for local users to manage the ADSL router. Notice that there is no IP address for the WAN interface and therefore remote technical support is not available when in bridge mode.

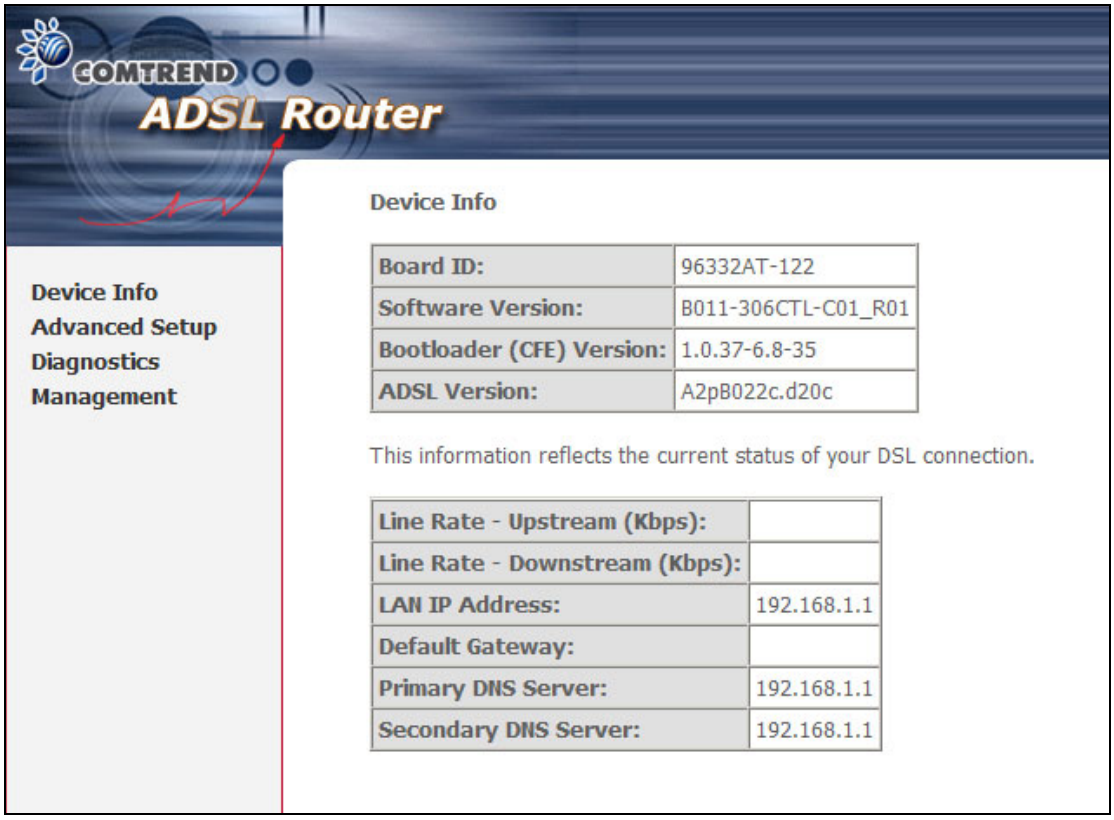
Step 3: Click **Next** to continue. The following screen will be displayed.


COMTREND
ADSL Router
WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
VPI / VCI: 0 / 35
Connection Type: Bridge
Service Name: br_0_35
Service Category: UBR
IP Address: Not Applicable
Service State: Enabled
NAT: Disabled
Firewall: Disabled
IGMP Multicast: Not Applicable
Quality Of Service: Enabled
Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.
Back
Save/Reboot
Device Info
Quick Setup
Advanced Setup
Diagnostics
Management

The WAN Setup-Summary screen presents the entire configuration summary. Click **Save/Reboot** if the settings are correct. Click **Back** to modify the settings.

Chapter 5 Device Information

This screen provides summary information about the device, ADSL and IP status.



NOTE:	The selections available on the main menu are based upon account settings and configured connections.

5.1 WAN

Click **Device Info** on the menu bar to display the WAN option. Then, click **WAN** on the Device Info menu bar to display the configured PVC(s) and the status.

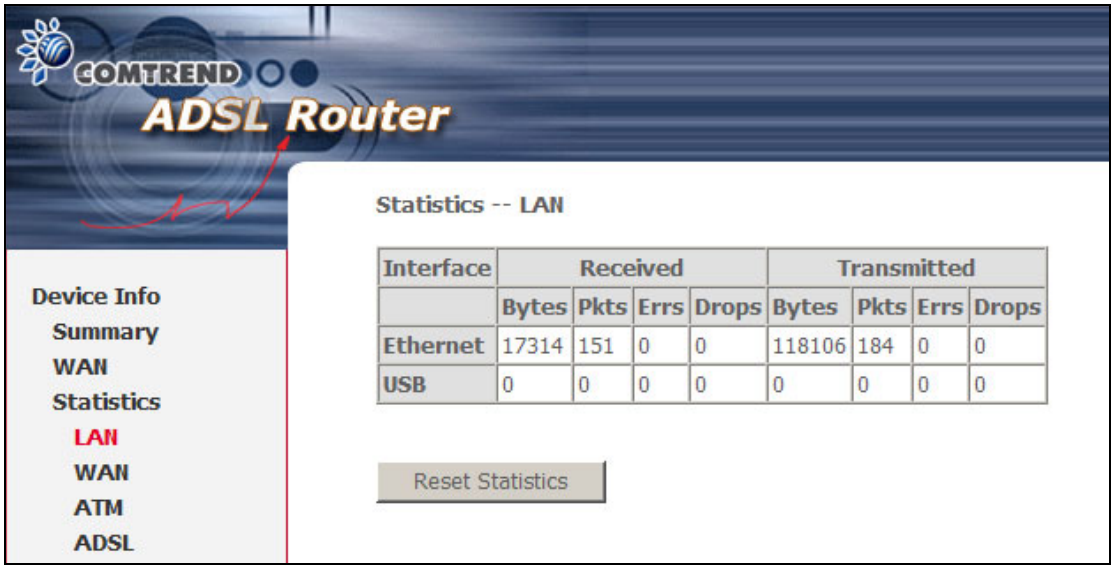
Heading	Description
VPI/VCI	Shows the values of the ATM VPI/VCI
Con. ID	Shows the connection ID
Category	Shows the ATM service classes
Service	Shows the name for WAN connection
Interface	Shows connection interfaces
Protocol	Shows the connection type, such as PPPoE, PPPoA, etc.
IGMP	Shows the statue of the IGMP function
QoS	Shows if QoS is enabled or disabled
State	Shows the connection state of the WAN connection
Status	Lists the status of DSL link
IP Address	Shows IP address for WAN interface

5.2 Statistics

Selection of the Statistics screen provides statistics for the Network Interface of LAN, WAN, ATM and ADSL. All statistics screens are updated every 15 seconds.

5.2.1 LAN Statistics

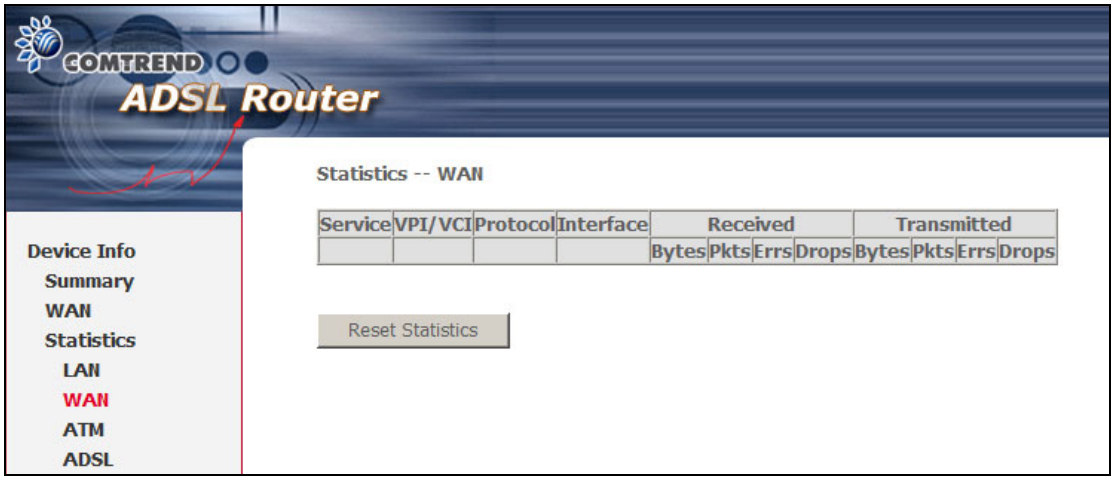
The Network Statistics screen shows interface statistics for Ethernet and USB interfaces. (The Network Statistics screen shows interface statistics for LAN of Ethernet and USB interfaces. This shows byte transfer, packet transfer, Error and Drop statistics for the LAN interface.)



Interface		Shows connection interfaces
Received/Transmitted	- Bytes	Rx/TX (receive/transmit) packet in bytes
	- Pkts	Rx/TX (receive/transmit) packets
	- Errs	Rx/TX (receive/transmit) packets with errors
	- Drops	Rx/TX (receive/transmit) packets dropped

5.2.2 WAN Statistics

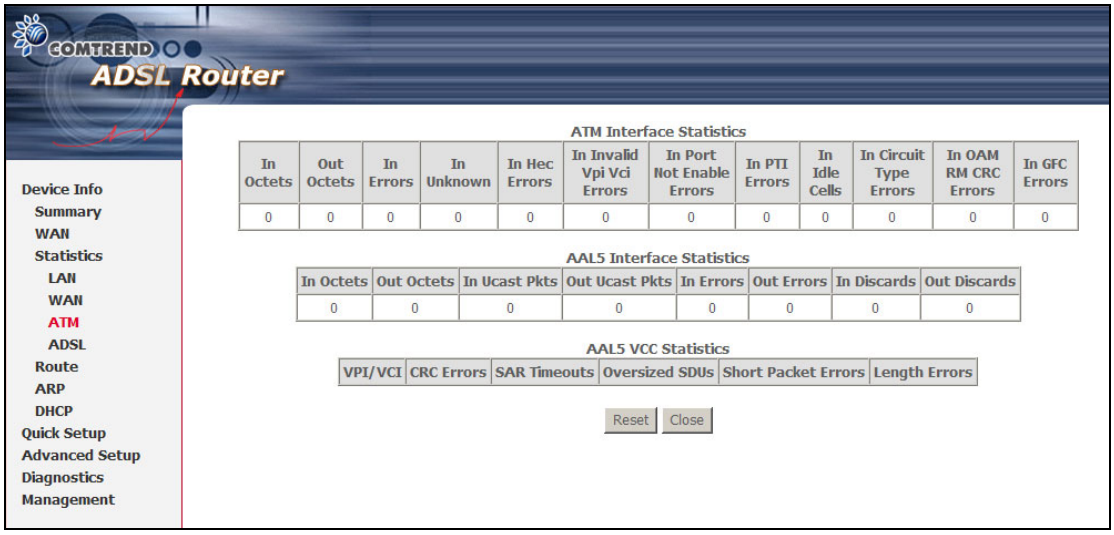
The following figure shows the WAN statistics screen.



Service		WAN service label
VPI/VCI		ATM Virtual Path/Channel Identifiers
Protocol		Connection type (e.g. PPPoE, IPoA, Bridge)
Interface		Shows connection interfaces in the following format: nas_(VPI number_VCI number). These interfaces are devised by the system and not the user.
Received/Transmitted	- Bytes	Rx/TX (receive/transmit) packet in bytes
	- Pkts	Rx/TX (receive/transmit) packets
	- Errs	Rx/TX (receive/transmit) packets with errors
	- Drops	Rx/TX (receive/transmit) packets dropped

5.2.3 ATM statistics

The following figure shows the ATM statistics screen.



ATM Interface Statistics

Field	Description
In Octets	Number of received octets over the interface
Out Octets	Number of transmitted octets over the interface
In Errors	Number of cells dropped due to uncorrectable HEC errors
In Unknown	Number of received cells discarded during cell header validation, including cells with unrecognized VPI/VCI values, and cells with invalid cell header patterns. If cells with undefined PTI values are discarded, they are also counted here.
In Hec Errors	Number of cells received with an ATM Cell Header HEX error
In Invalid Vpi Vci Errors	Number of cells received with an unregistered VCC address.
In Port Not Enable Errors	Number of cells received on a port that has not been enabled.
In PTI Errors	Number of cells received with an ATM header Payload Type Indicator (PTI) error
In Idle Cells	Number of idle cells received
In Circuit Type Errors	Number of cells received with an illegal circuit type
In OAM RM CRC Errors	Number of OAM and RM cells received with CRC errors
In GFC Errors	Number of cells received with a non-zero GFC.

AAL5 Interface Statistics

Field	Description
In Octets	Number of received AAL5/AAL0 CPCS PDU octets
Out Octets	Number of received AAL5/AAL0 CPCS PDUs octets transmitted
In Ucast Pkts	Number of received AAL5/AAL0 CPCS PDUs passed to a higher-layer for transmission
Out Ucast Pkts	Number of received AAL5/AAL0 CPCS PDUs received from

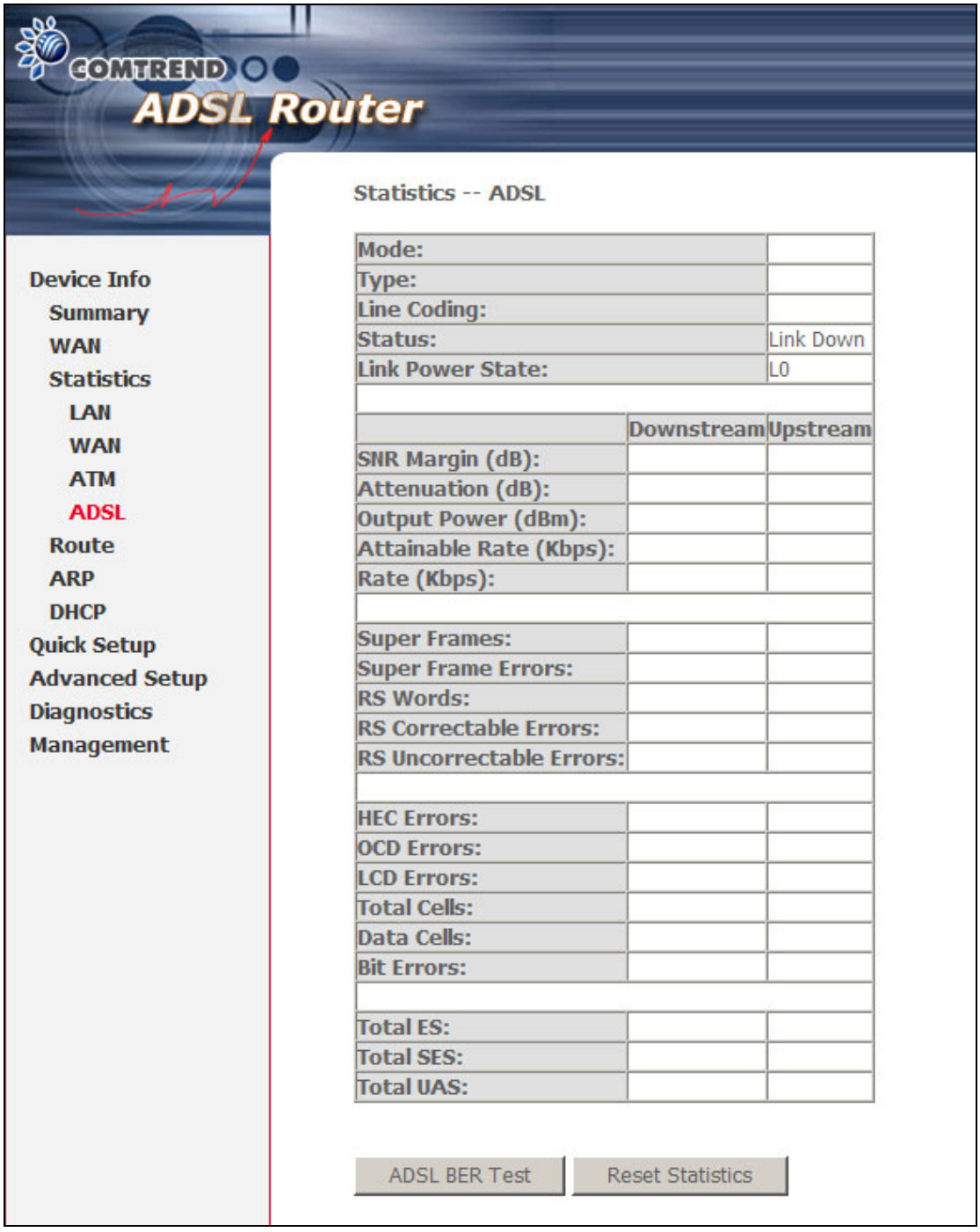
	a higher layer for transmissions
In Errors	Number of received AAL5/AAL0 CPCS PDUs received that contain an error. The types of errors counted include CRC-32 errors.
Out Errors	Number of received AAL5/AAL0 CPCS PDUs that could be transmitted due to errors.
In Discards	Number of received AAL5/AAL0 CPCS PDUs discarded due to an input buffer overflow condition.
Out Discards	This field is not currently used

AAL5 VCC Statistics

Field	Descriptions
VPI/VCI	ATM Virtual Path/Channel Identifiers
CRC Errors	Number of PDUs received with CRC-32 errors
SAR TimeOuts	Number of partially re-assembled PDUs, which were discarded because they were not fully re-assembled within the required period of time. If the re-assembly time is not supported then, this object contains a zero value.
Oversized SDUs	Number of PDUs discarded because the corresponding SDU was too large
Short Packets Errors	Number of PDUs discarded because the PDU length was less than the size of the AAL5 trailer
Length Errors	Number of PDUs discarded because the PDU length did not match the length in the AAL5 trailer

5.2.4 ADSL Statistics

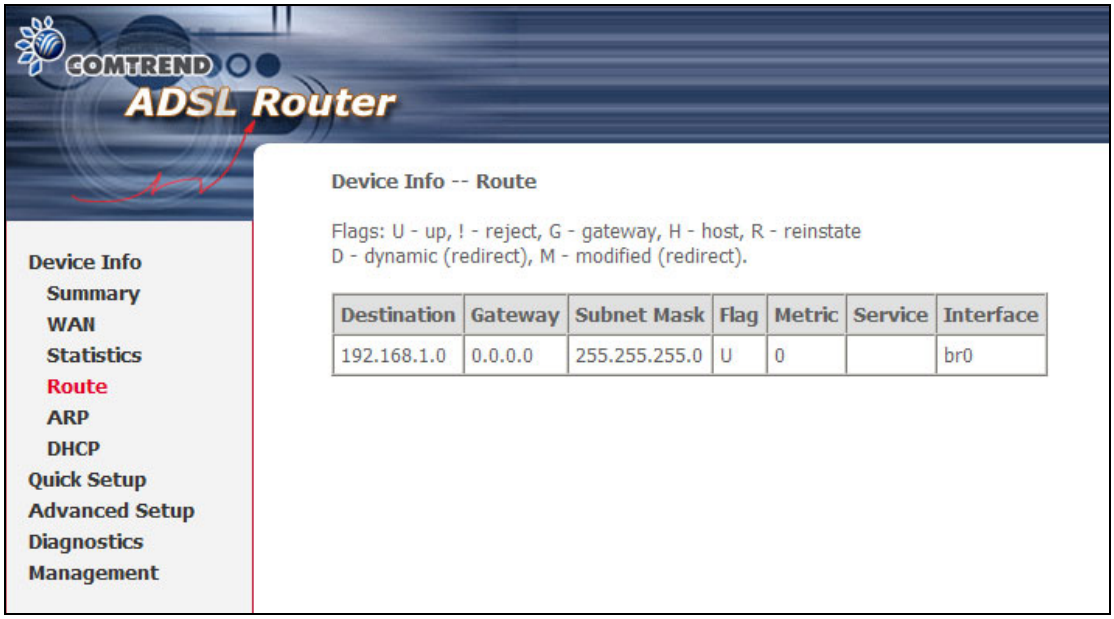
The following figure shows the ADSL Statistics screen. Within the ADSL Statistics window, a Bit Error Rate Test can be or statistics refreshed with the Reset button.


COMTREND
ADSL Router
Device Info
Summary
WAN
Statistics
LAN
WAN
ATM
ADSL
Route
ARP
DHCP
Quick Setup
Advanced Setup
Diagnostics
Management
Statistics -- ADSL
Mode:
Type:
Line Coding:
Status: Link Down
Link Power State: L0
Downstream
Upstream
SNR Margin (dB):
Attenuation (dB):
Output Power (dBm):
Attainable Rate (Kbps):
Rate (Kbps):
Super Frames:
Super Frame Errors:
RS Words:
RS Correctable Errors:
RS Uncorrectable Errors:
HEC Errors:
OCD Errors:
LCD Errors:
Total Cells:
Data Cells:
Bit Errors:
Total ES:
Total SES:
Total UAS:
ADSL BER Test
Reset Statistics

Field	Description
Mode	Modulation protocol G.dmt, G.lite, T1.413, ADSL2, ADSL2+
Type	Channel type Interleave or Fast
Line Coding	Trellis On/Off
Status	Lists the status of the DSL link
Link Power State	Link output power state.
SNR Margin (dB)	Signal to Noise Ratio (SNR) margin
Attenuation (dB)	Estimate of average loop attenuation in the downstream direction.
Output Power (dBm)	Total upstream output power
Attainable Rate (Kbps)	The sync rate you would obtain.
Rate (Kbps)	Current sync rate.
Super Frames	Total number of super frames
Super Frame Errors	Number of super frames received with errors
RS Words	Total number of Reed-Solomon code errors
RS Correctable Errors	Total Number of RS with correctable errors
RS Uncorrectable Errors	Total Number of RS words with uncorrectable errors
HEC Errors	Total Number of Header Error Checksum errors
OCD Errors	Total Number of out-of-cell Delineation errors
LCD Errors	Total number of Loss of Cell Delineation
Total Cells	Total number of ATM cells (including idle and data cells)
Data Cells	Total number of ATM data cells
Bit Errors	Total number of bit errors
Total ES:	Total Number of Errored Seconds
Total SES:	Total Number of Severely Errored Seconds
Total UAS:	Total Number of Unavailable Seconds

5.3 Route

Choose **Route** to display the routes that the router has found.



5.4 ARP

Click **ARP** to display the ARP information.

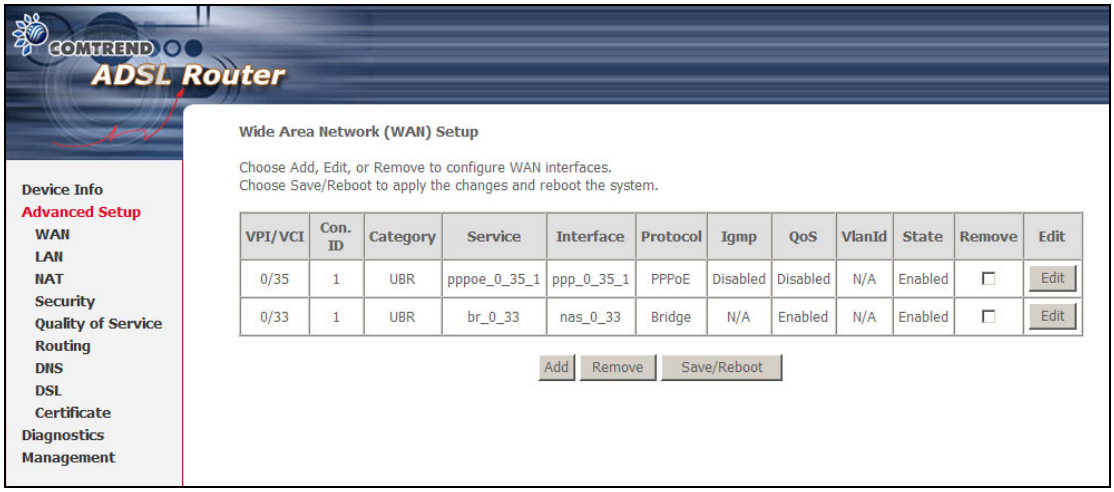
5.5 DHCP

Click **DHCP** to display the DHCP information.

Chapter 6 Advanced Setup

This chapter explains the advanced setup functions available from this submenu.

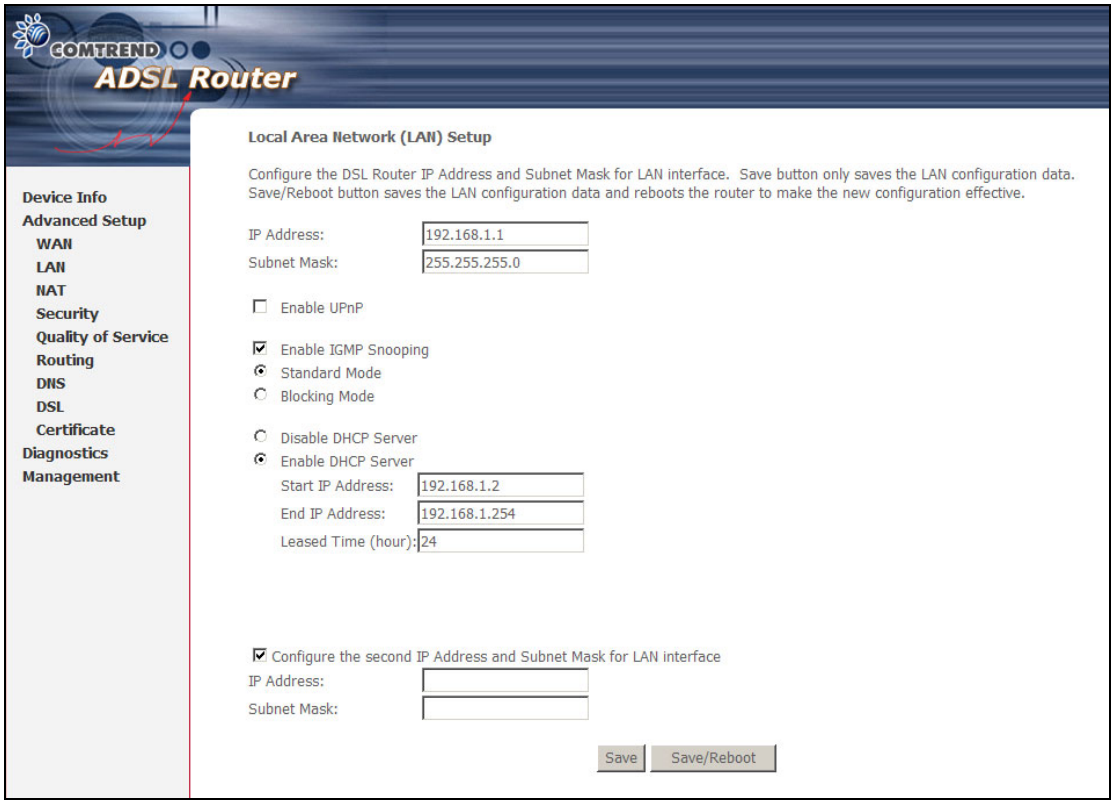
6.1 WAN



Heading	Information
VPI/VCI	ATM VPI (0-255) / VCI (32-65535)
Con. ID	WAN connection ID number
Category	ATM service category
Service	Name of the WAN connection
Interface	Name of the interface for WAN
Protocol	Shows the connection type
Igmp	Shows enable or disable IGMP proxy
QoS	Shows if IP QoS is enabled or disabled
VlanId	VLAN ID is used for VLAN Tagging (IEEE 802.1Q)
State	Shows the connection state of the WAN connection
Remove	Used to select connections for removal
Edit	Used to edit connections

6.2 LAN

Configure the DSL Router IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. Save/Reboot button saves the LAN configuration data and reboots the router to make the new configuration effective.



NOTE: NAT is enabled so **UPnP** is shown above (see underlined notes below).

Consult the field descriptions below for more details.

IP Address: Enter the IP address for the LAN port.

Subnet Mask: Enter the subnet mask for the LAN port.

Enable UPnP: Tick the box to enable Universal Plug and Play.
This option is hidden when NAT disabled or if no PVC exists

Enable IGMP Snooping: Enable by ticking the box.

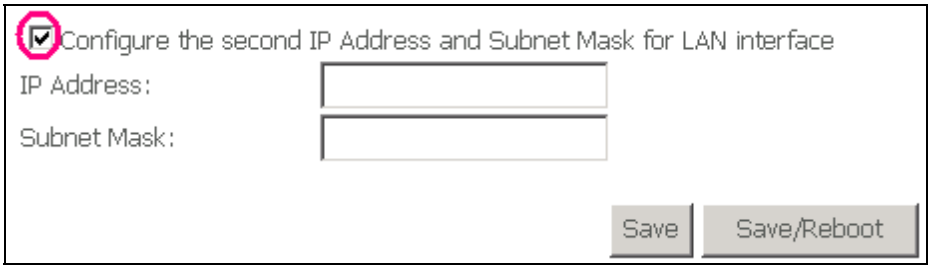
Standard Mode**:** In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group – even if IGMP snooping is enabled.

Blocking Mode**:** In blocking mode, the multicast data traffic will be blocked and not flood to all bridge ports when there are no client subscriptions to any multicast group.

DHCP Server: To enable DHCP, select **Enable DHCP server** and enter starting and ending IP addresses and the leased time. This setting configures the router to automatically assign IP, default gateway and DNS server addresses to every PC on your LAN.

DHCP Server Relay: Enable with checkbox and enter DHCP Server IP address. This allows the Router to relay the DHCP packets to the remote DHCP server. The remote DHCP server will provide the IP address. *This option is hidden if NAT is enabled*

To configure a secondary IP address for the LAN port, tick the checkbox below.



IP Address: Enter the secondary IP address for the LAN port.

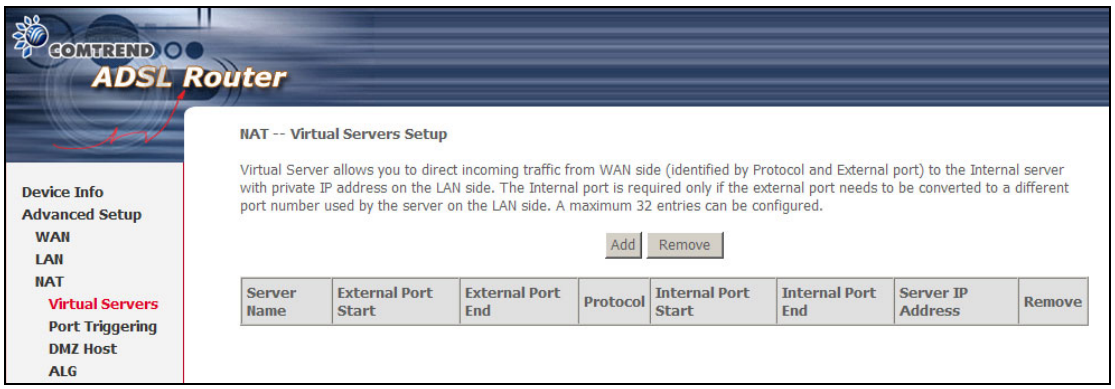
Subnet Mask: Enter the secondary subnet mask for the LAN port.

6.3 NAT

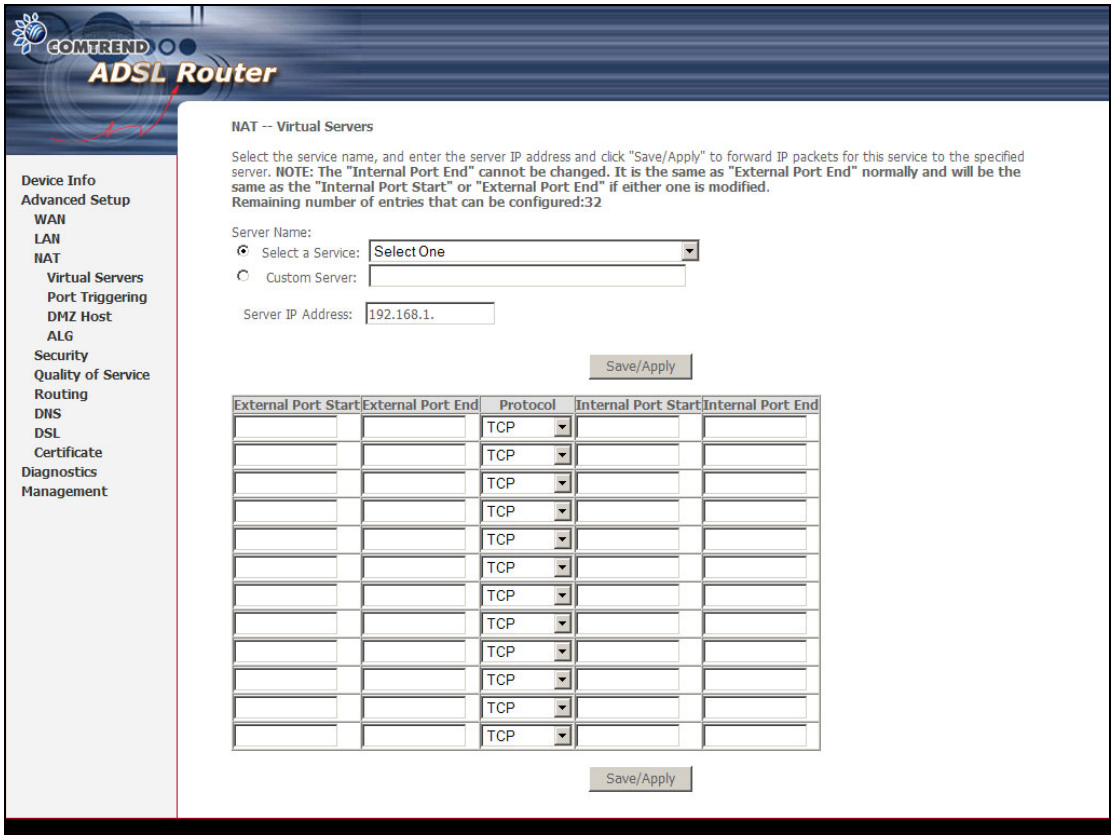
To display the NAT function, you must enable the NAT feature in the WAN Setup.

6.3.1 Virtual Servers

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.


COMTREND
ADSL Router
Device Info
Advanced Setup
WAN
LAN
NAT
Virtual Servers
Port Triggering
DMZ Host
ALG
NAT -- Virtual Servers Setup
Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.
Add
Remove
Server Name
External Port Start
External Port End
Protocol
Internal Port Start
Internal Port End
Server IP Address
Remove

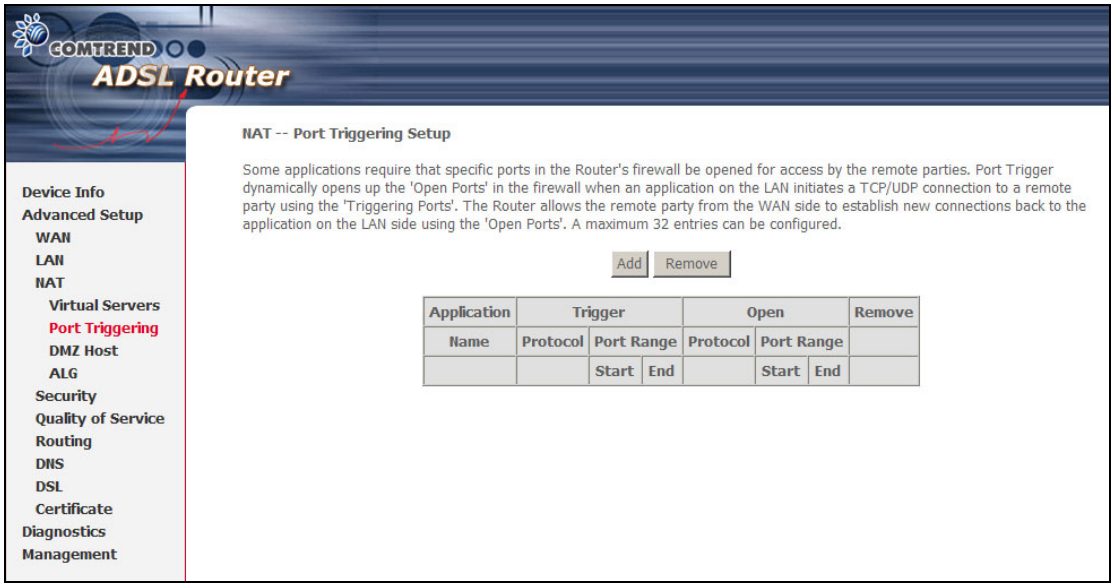
To add a Virtual Server, click the **Add** button. The following screen will display.



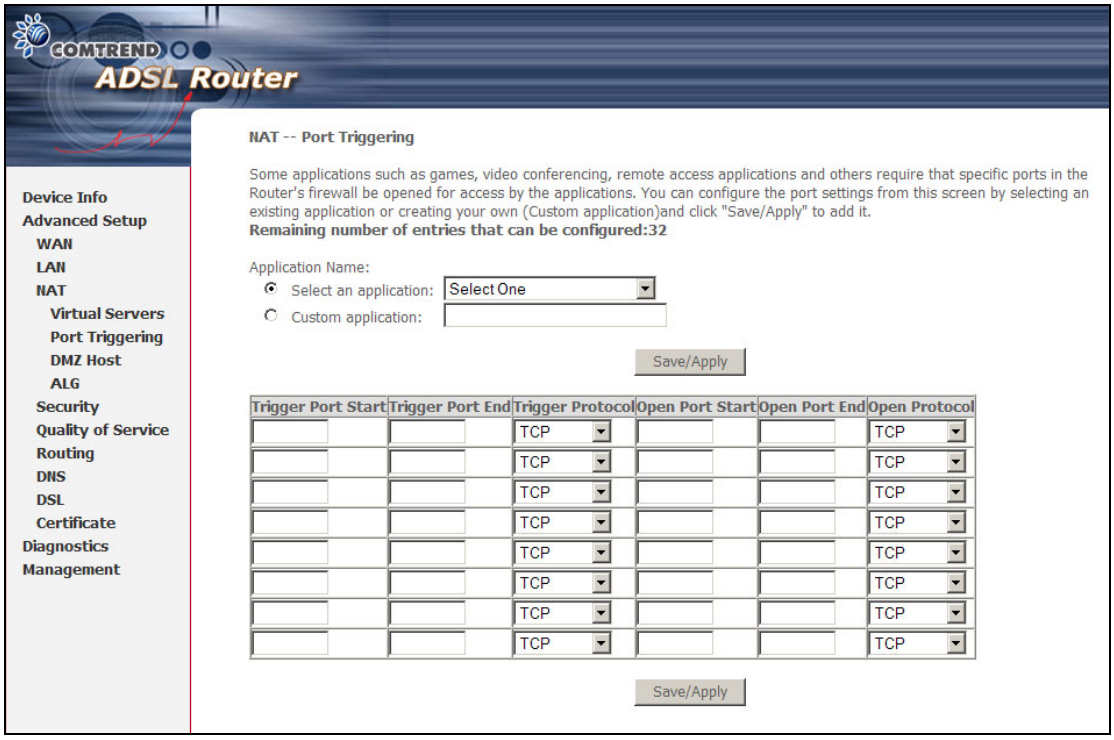
Select a Service Or Custom Server	User should select the service from the list. Or User can enter the name of their choice.
Server IP Address	Enter the IP address for the server.
External Port Start	Enter the starting external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
External Port End	Enter the ending external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
Protocol	User can select from: TCP, TCP/UDP or UDP.
Internal Port Start	Enter the internal port starting number (when you select Custom Server). When a service is selected the port ranges are automatically configured
Internal Port End	Enter the internal port ending number (when you select Custom Server). When a service is selected the port ranges are automatically configured.

6.3.2 Port Triggering

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.



To add a Trigger Port, click the **Add** button. The following screen will display.

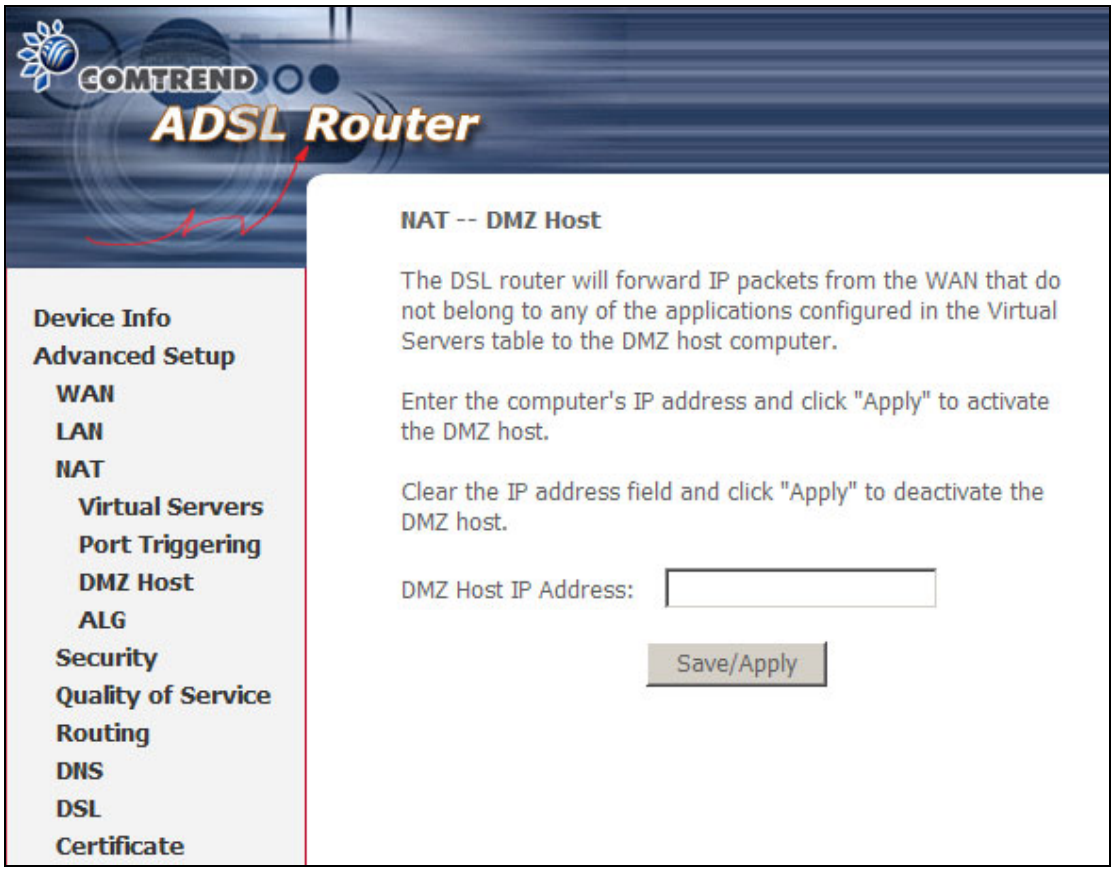


Select an Application Or Custom Application	User should select the application from the list. Or User can enter the name of their choice.
Trigger Port Start	Enter the starting trigger port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Trigger Port End	Enter the ending trigger port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Trigger Protocol	User can select from: TCP, TCP/UDP or UDP.
Open Port Start	Enter the starting open port number (when you select

	custom application). When an application is selected the port ranges are automatically configured.
Open Port End	Enter the ending open port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Open Protocol	User can select from: TCP, TCP/UDP or UDP.

6.3.3 DMZ Host

The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

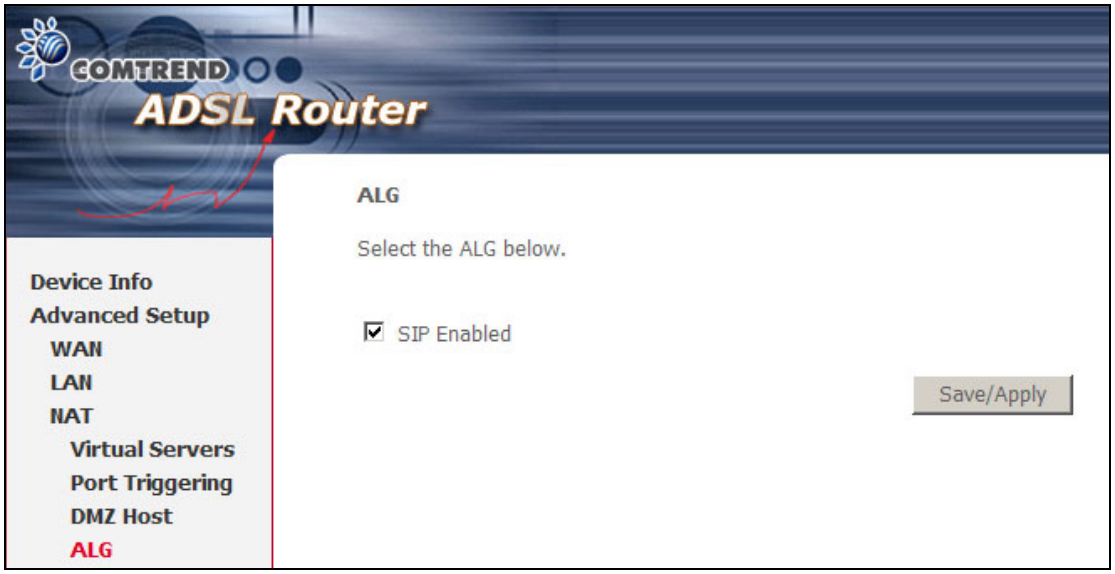


Enter the computer's IP address and click **Apply** to activate the DMZ host.

Clear the IP address field and click **Apply** to deactivate the DMZ host.

6.3.4 ALG

SIP ALG is Application layer gateway. If the user has an IP phone(SIP) or VoIP gateway(SIP) behind the ADSL router, the SIP ALG can help VoIP packet passthrough the router (NAT enabled).



NOTE: SIP (Session Initiation Protocol, RFC3261) is the protocol of choice for most VoIP (Voice over IP) phones to initiate communication. This ALG is only valid for SIP protocol running UDP port 5060.

6.4 Security

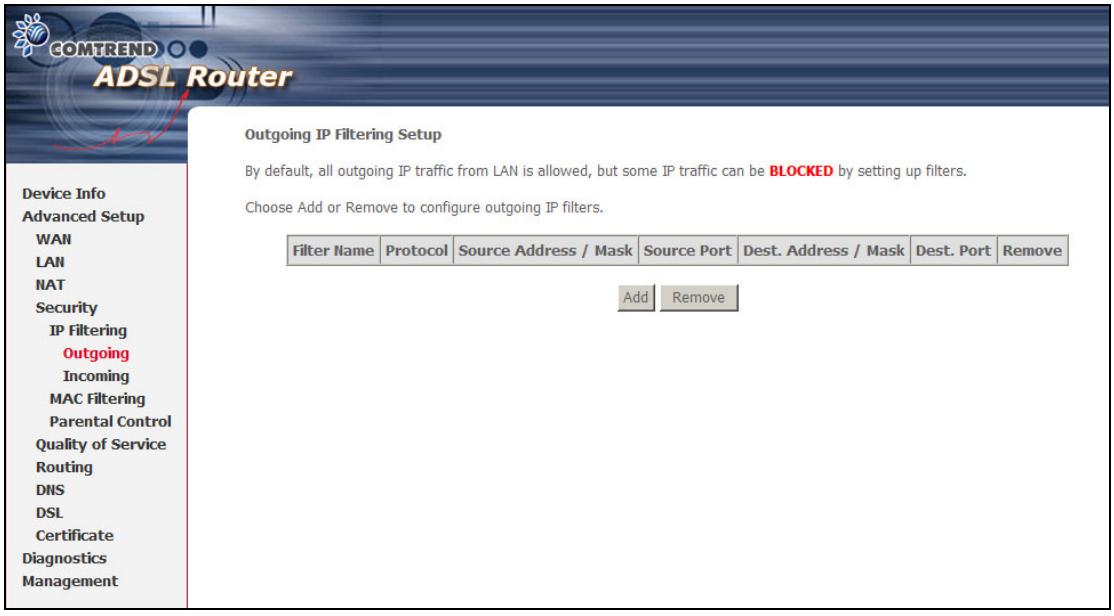
To display this function, you must enable the firewall feature in WAN Setup. For detailed descriptions with examples please consult Appendix D: Security

6.4.1 IP Filtering

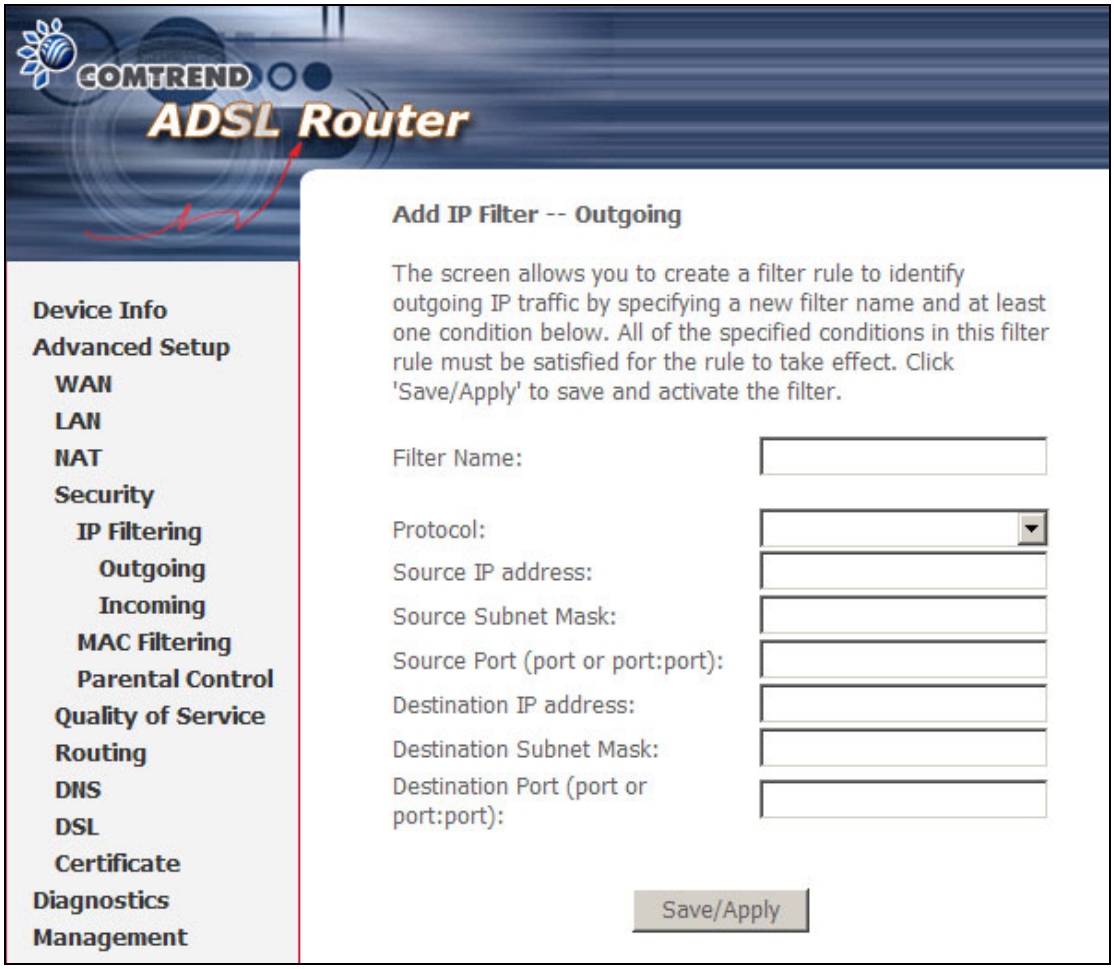
IP filtering allows you to create a filter rule to identify outgoing/incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.

OUTGOING IP FILTER

To add a filtering rule, click the **Add** button on the screen below.



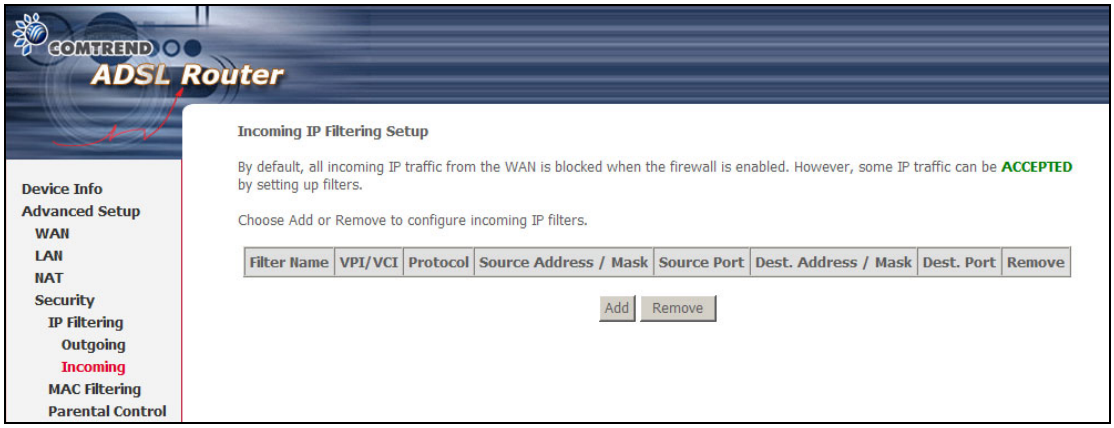
NOTE: The default setting for Outgoing is Accepted.



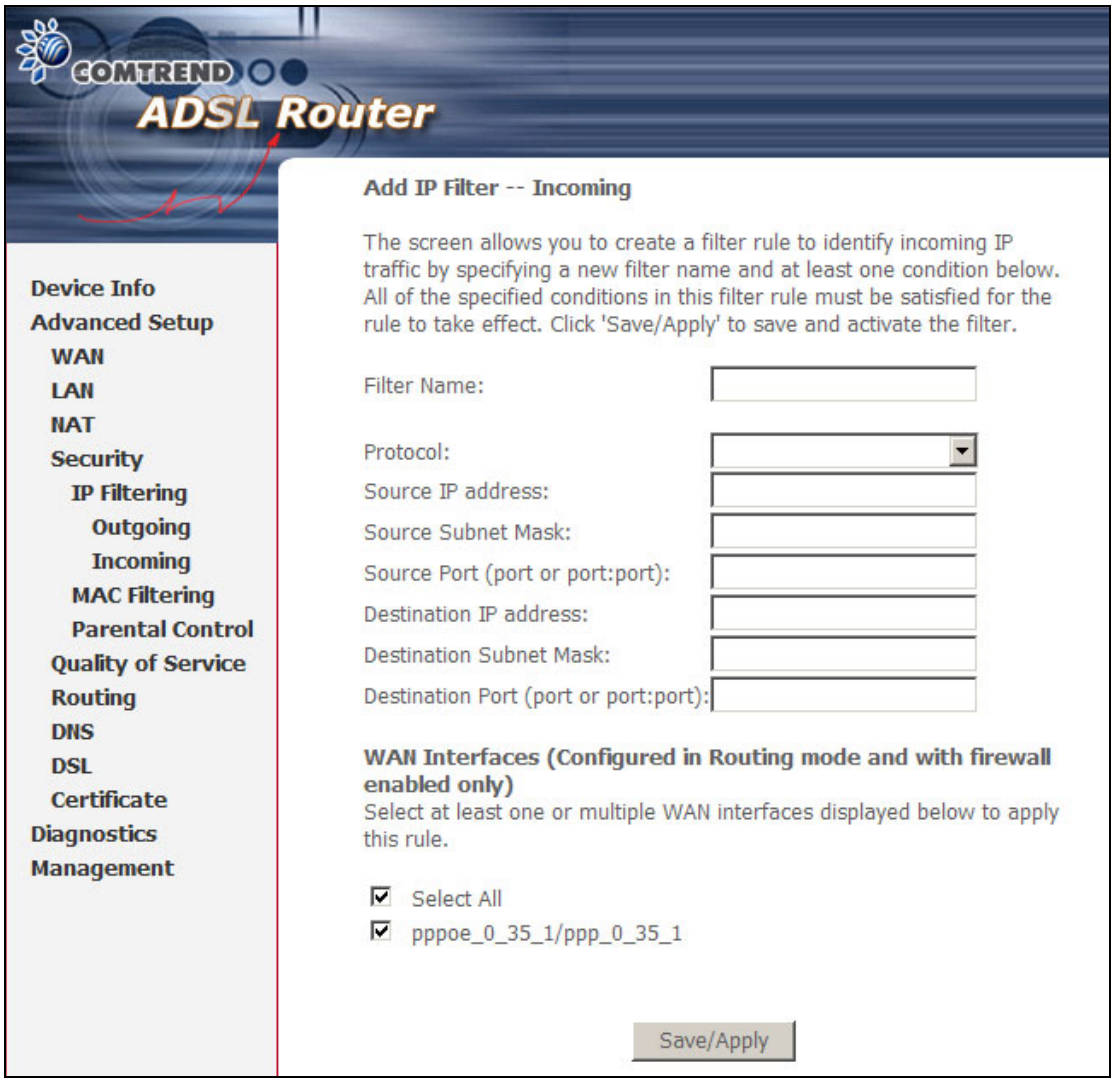
Field	Description
Filter Name	Type a name for the filter rule.
Protocol	User can select from: TCP, TCP/UDP, UDP or ICMP
Source IP address	Enter source IP address.
Source Subnet Mask	Enter source subnet mask.
Source Port (port or port:port)	Enter source port number.
Destination IP address	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
Destination port (port or port:port)	Enter destination port number.

INCOMING IP FILTER

To add a filtering rule, click the **Add** button on the screen below.



NOTE: The default setting for Incoming is Blocked.


COMTREND
ADSL Router
Add IP Filter -- Incoming
The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.
Filter Name:
Protocol:
Source IP address:
Source Subnet Mask:
Source Port (port or port:port):
Destination IP address:
Destination Subnet Mask:
Destination Port (port or port:port):
WAN Interfaces (Configured in Routing mode and with firewall enabled only)
Select at least one or multiple WAN interfaces displayed below to apply this rule.
Select All
pppoe_0_35_1/ppp_0_35_1
Save/Apply
Device Info
Advanced Setup
WAN
LAN
NAT
Security
IP Filtering
Outgoing
Incoming
MAC Filtering
Parental Control
Quality of Service
Routing
DNS
DSL
Certificate
Diagnostics
Management

Field	Description
Filter Name	Type a name for the filter rule.
Protocol	User can select from: TCP, TCP/UDP, UDP or ICMP
Source IP address	Enter source IP address.
Source Subnet Mask	Enter source subnet mask.

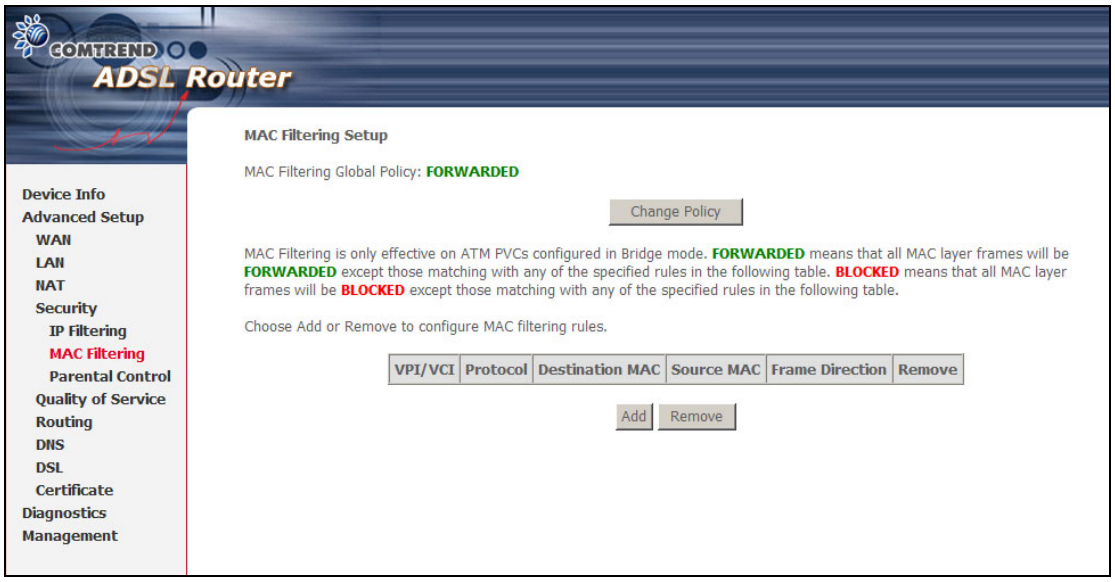
Source Port (port or port:port)	Enter source port number.
Destination IP address	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
Destination port (port or port:port)	Enter destination port number.

6.4.2 MAC Filtering

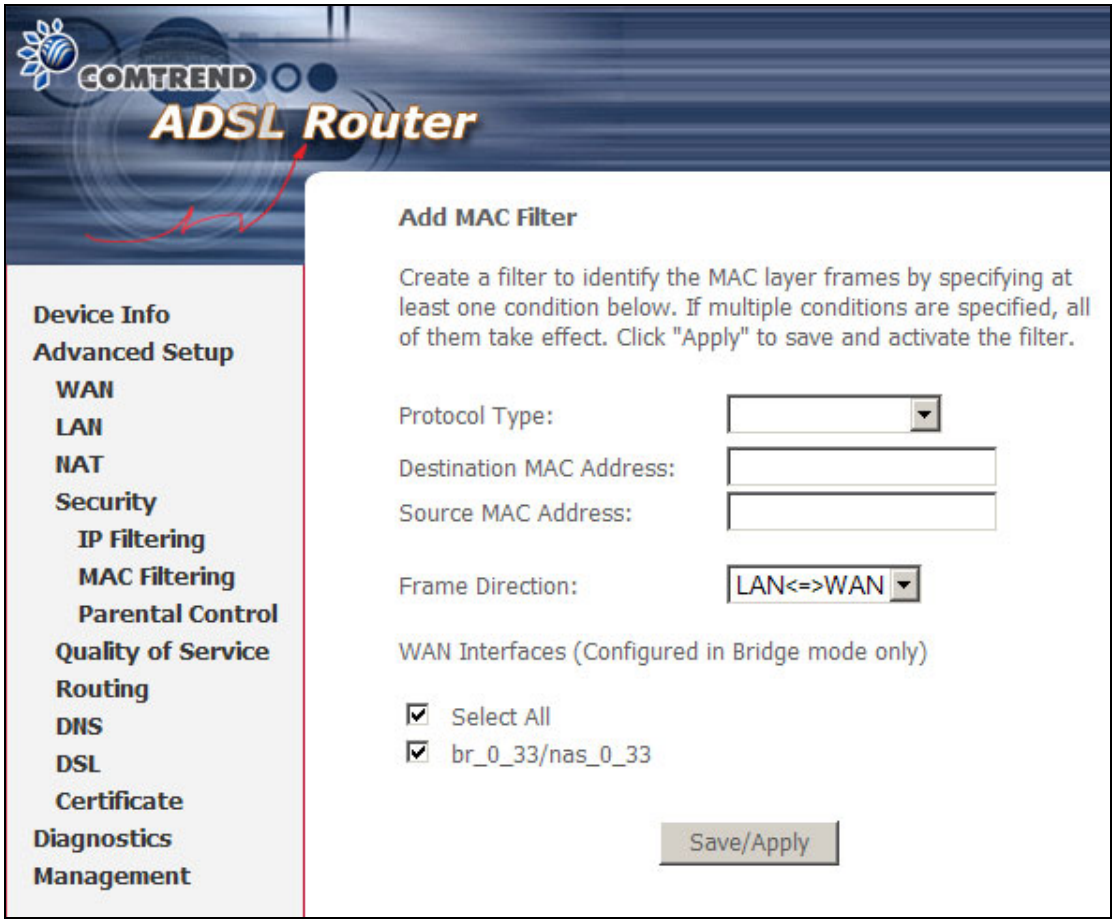
NOTE:	This function is only available when in bridge mode. PPPoE, PPPoA, IPoA and MER use IP Filtering (pg. 49) to perform a similar function.

Each network device has a unique 48-bit MAC address. This can be used to filter (block or forward) packets based on the originating device. MAC filtering policy and rules for the CT-5611TC can be set according to the following procedure.

The policy **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching the rules specified in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching the rules specified in the following table. The default policy is **FORWARDED**. This can be changed by clicking the **Change Policy** button.



Choose **Add** or **Remove** to configure MAC filtering rules. The following screen will appear when you click **Add**. Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them must be met. Click **Save/Apply** to save and activate the filter rule.

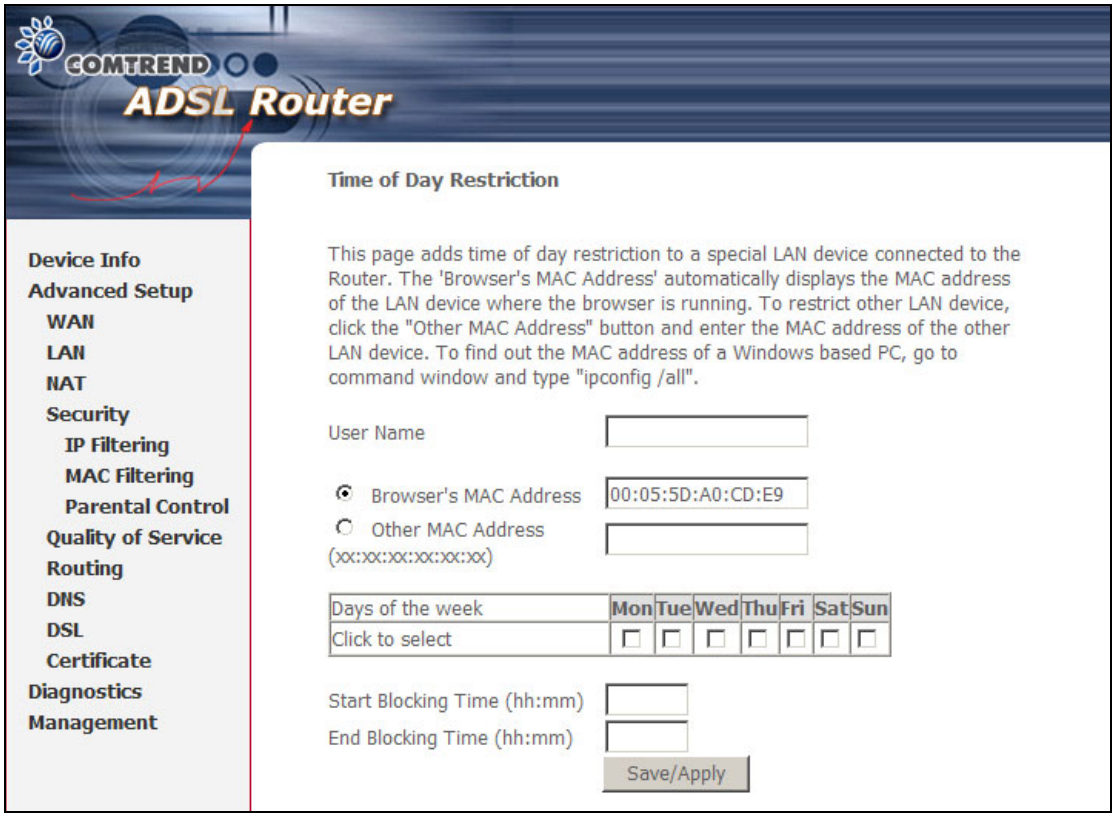


Field	Description
Protocol Type	PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP
Destination MAC Address	Defines the destination MAC address
Source MAC Address	Defines the source MAC address
Frame Direction	Select the incoming/outgoing packet interface
WAN Interfaces	Applies filter to selected PVCs (bridge mode only). Filter rules are arranged according to PVC, as shown under the VPI/VCI heading on the previous screen.

6.4.3 Parental Control

Parental control allows parents, schools, and libraries to set access times for Internet use. To add a parental control, click the **Add** button.

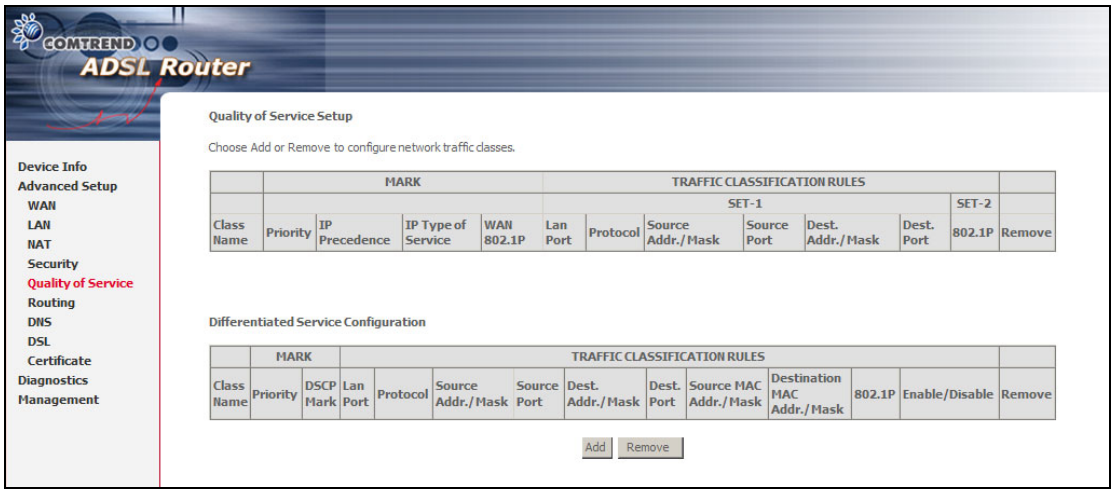
The following screen will display.


COMTREND
ADSL Router
Time of Day Restriction
This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".
Device Info
Advanced Setup
WAN
LAN
NAT
Security
IP Filtering
MAC Filtering
Parental Control
Quality of Service
Routing
DNS
DSL
Certificate
Diagnostics
Management
User Name
Browser's MAC Address
00:05:5D:A0:CD:E9
Other MAC Address
(xx:xx:xx:xx:xx:xx)
Days of the week
Mon Tue Wed Thu Fri Sat Sun
Click to select
Start Blocking Time (hh:mm)
End Blocking Time (hh:mm)
Save/Apply

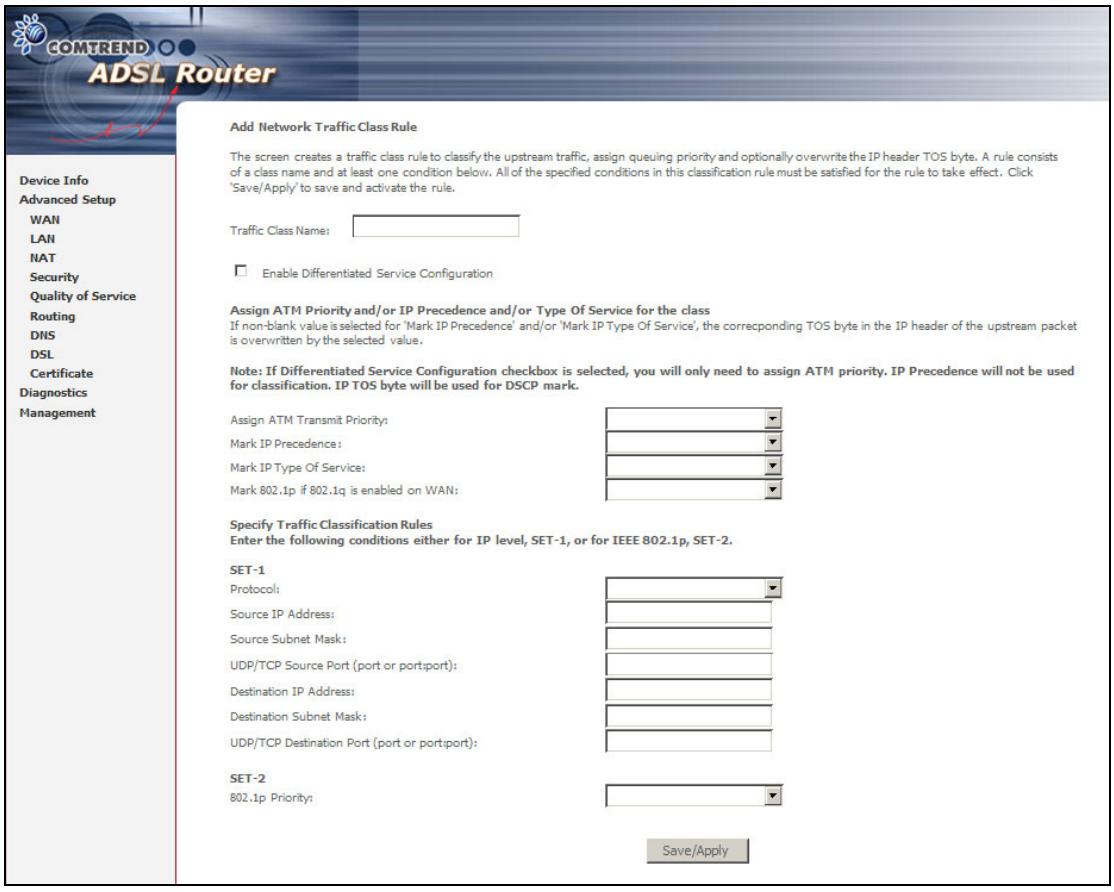
Username	To set access Internet user name
MAC Address	To set what MAC to access Internet
Days of the week	To set what day can be access Internet
Start/Stop Blocking Time	To set time range for Internet Blocking

6.5 Quality of Service

To display the Security function, you must enable QoS in WAN Setup.



Choose **Add** to configure network traffic classes. The following screen will display.


COMTREND
ADSL Router
Add Network Traffic Class Rule
The screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.
Traffic Class Name:
Enable Differentiated Service Configuration
Assign ATM Priority and/or IP Precedence and/or Type Of Service for the class
If non-blank value is selected for 'Mark IP Precedence' and/or 'Mark IP Type Of Service', the correcponding TOS byte in the IP header of the upstream packet is overwritten by the selected value.
Note: If Differentiated Service Configuration checkbox is selected, you will only need to assign ATM priority. IP Precedence will not be used for classification. IP TOS byte will be used for DSCP mark.
Assign ATM Transmit Priority:
Mark IP Precedence:
Mark IP Type Of Service:
Mark 802.1p if 802.1q is enabled on WAN:
Specify Traffic Classification Rules
Enter the following conditions either for IP level, SET-1, or for IEEE 802.1p, SET-2.
SET-1
Protocol:
Source IP Address:
Source Subnet Mask:
UDP/TCP Source Port (port or port:port):
Destination IP Address:
Destination Subnet Mask:
UDP/TCP Destination Port (port or port:port):
SET-2
802.1p Priority:
Save/Apply
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
DNS
DSL
Certificate
Diagnostics
Management

Traffic Class Name	Enter name for traffic class
Assign ATM Transmit Priority	Select Low, Medium or High.
Mark IP Precedence	Select between 1-7. The lower the digit shows the higher the priority
Mark IP Type Of Service	Select either: Normal Service, Minimize Cost,

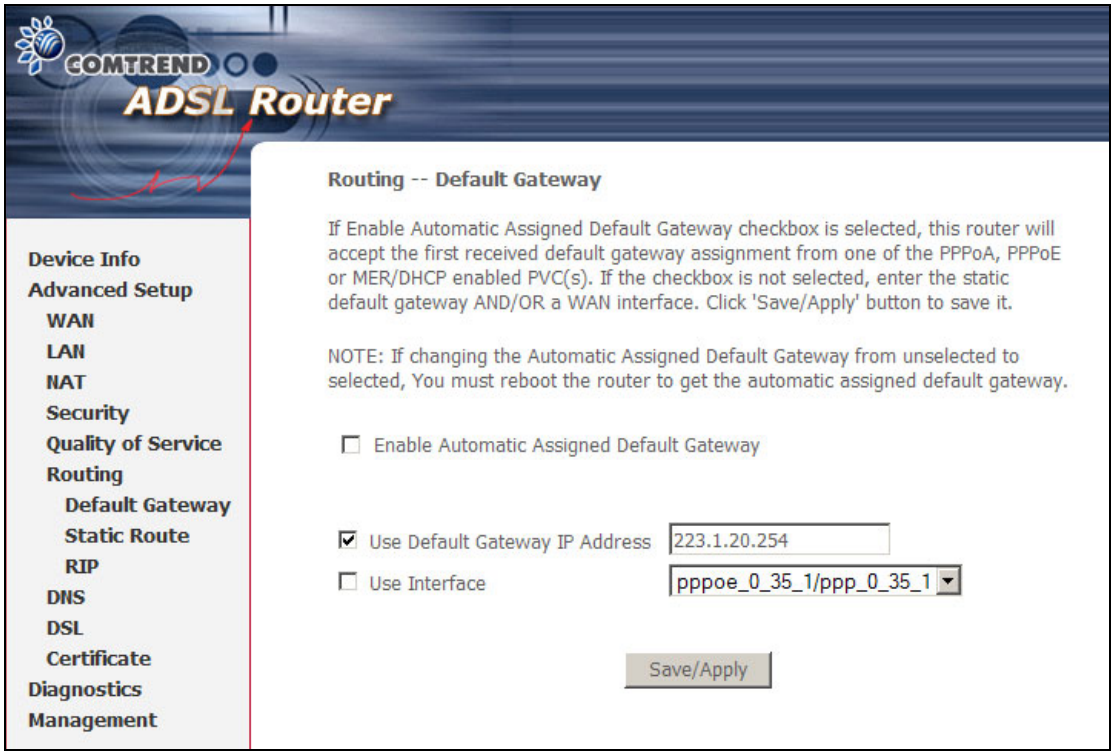
	Maximize Reliability, Maximize Throughput, Minimize Delay
Mark 802.1p if 802.1q is enabled on WAN	Select between 1-7. The lower the digit shows the higher the priority
Physical LAN Port	User can select from: ENET, ENET(1-4), USB or Wireless.
Protocol	User can select from: TCP, TCP/UDP, UDP or ICMP.
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the subnet mask for the source IP address.
UDP/TCP Source Port (port or port:port)	Enter source port number.
Destination IP address	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
UDP/TCP Destination port (port or port:port)	Enter destination port number.
802.1p Priority	Select between 0-7. The lower the digit shows the higher the priority

6.6 Routing

The Routing dialog box allows you to configure Default gateway and Static Route.

6.6.1 Default Gateway

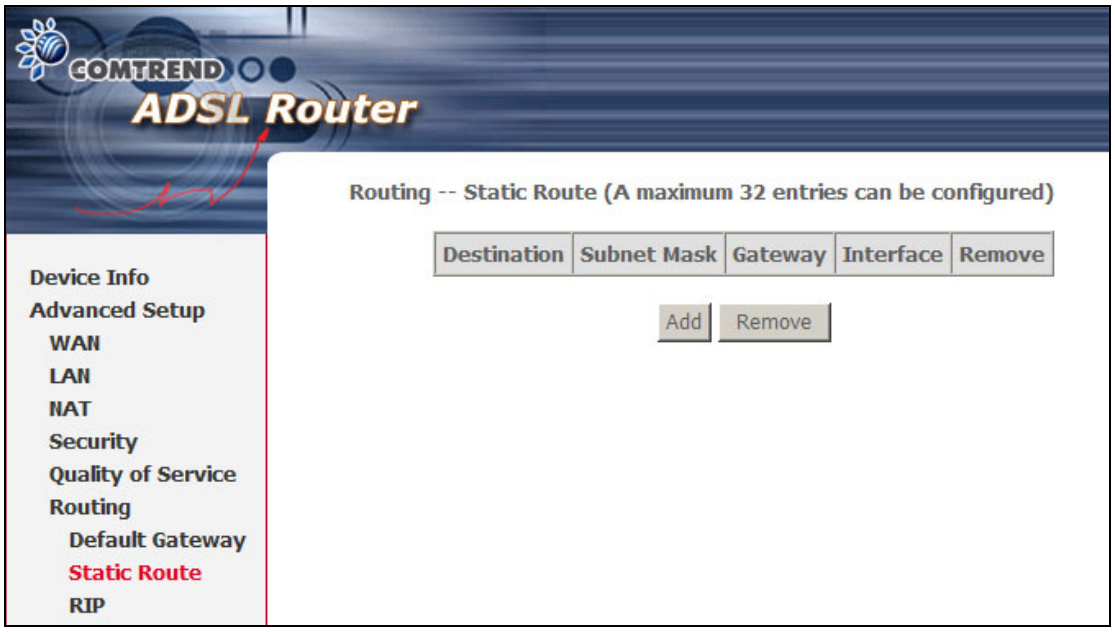
If **Enable Automatic Assigned Default Gateway** checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click **Save/Apply** button to save it.


COMTREND
ADSL Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
Default Gateway
Static Route
RIP
DNS
DSL
Certificate
Diagnostics
Management
Routing -- Default Gateway
If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click 'Save/Apply' button to save it.
NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.
Enable Automatic Assigned Default Gateway
Use Default Gateway IP Address
223.1.20.254
Use Interface
pppoe_0_35_1/ppp_0_35_1
Save/Apply

NOTE: After enabling Automatic Assigned Default Gateway, the router must be enabled to get the automatic assigned default gateway.

6.6.2 Static Route

Choose **Static Route** to display the Static Route screen. The Static Route screen lists the configured static routes, and allows configuring static routes. Choose **Add** or **Remove** to configure the static routes.

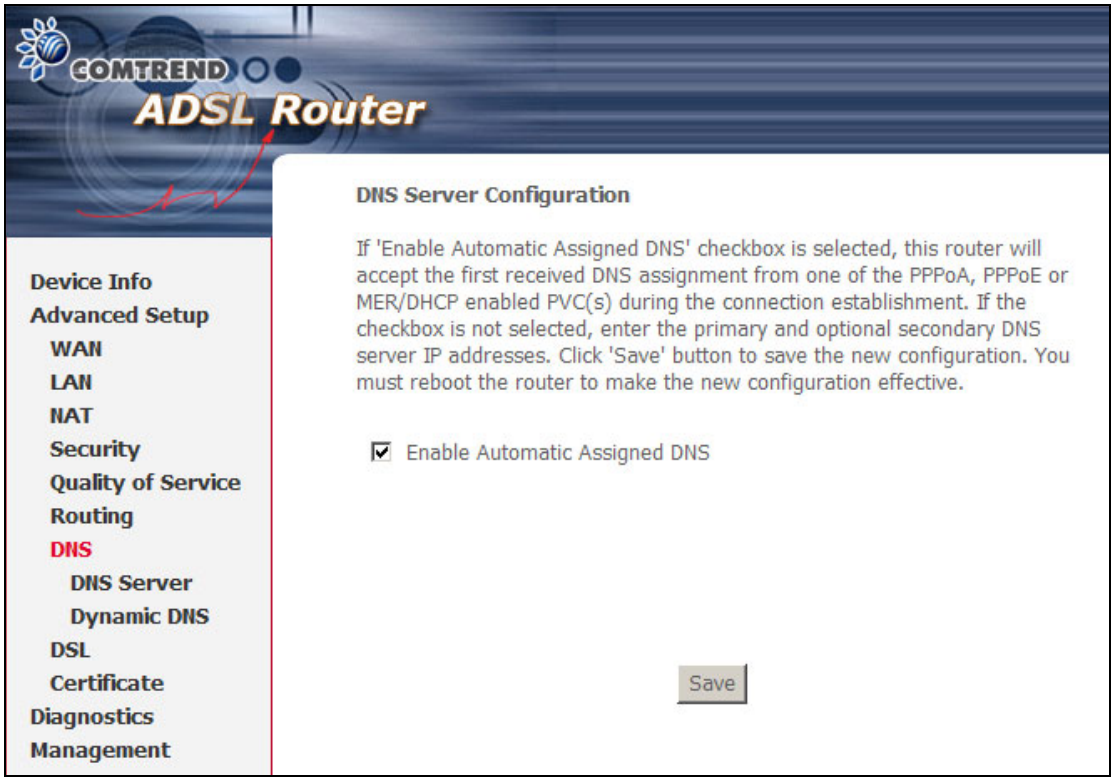


To add static route, click the **Add** button to display the following screen. Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click **Save/Apply** to add the entry to the routing table.

6.7 DNS

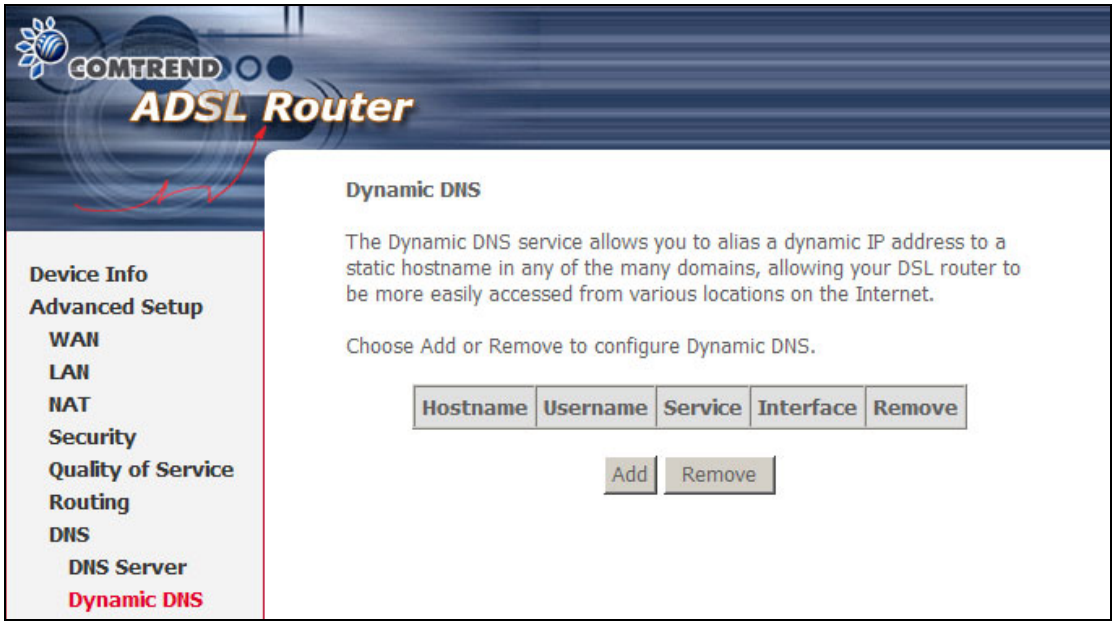
6.7.1 DNS Server

If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click 'Save' button to save the new configuration. You must reboot the router to make the new configuration effective.

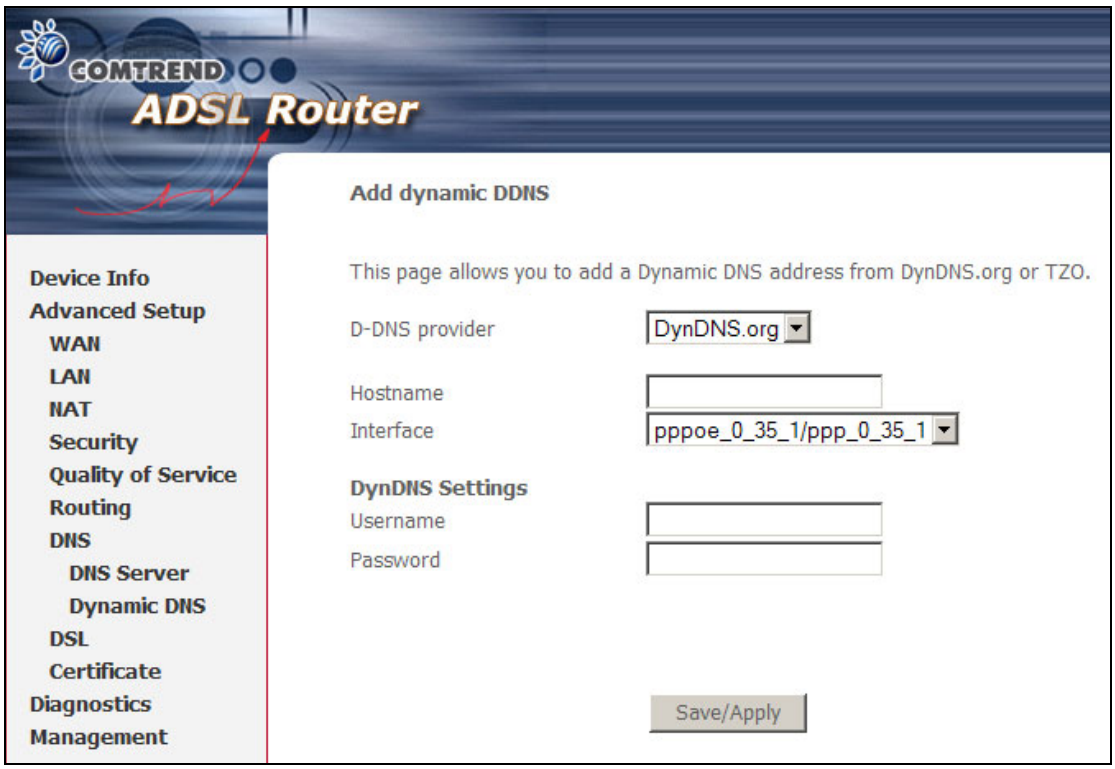

COMTREND
ADSL Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
DNS
DNS Server
Dynamic DNS
DSL
Certificate
Diagnostics
Management
DNS Server Configuration
If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click 'Save' button to save the new configuration. You must reboot the router to make the new configuration effective.
Enable Automatic Assigned DNS
Save

6.7.2 Dynamic DNS

The Dynamic DNS service allows you to map a dynamic IP address to a static hostname in any of the many domains, allowing your DSL router to be more easily accessed from various locations on the Internet.



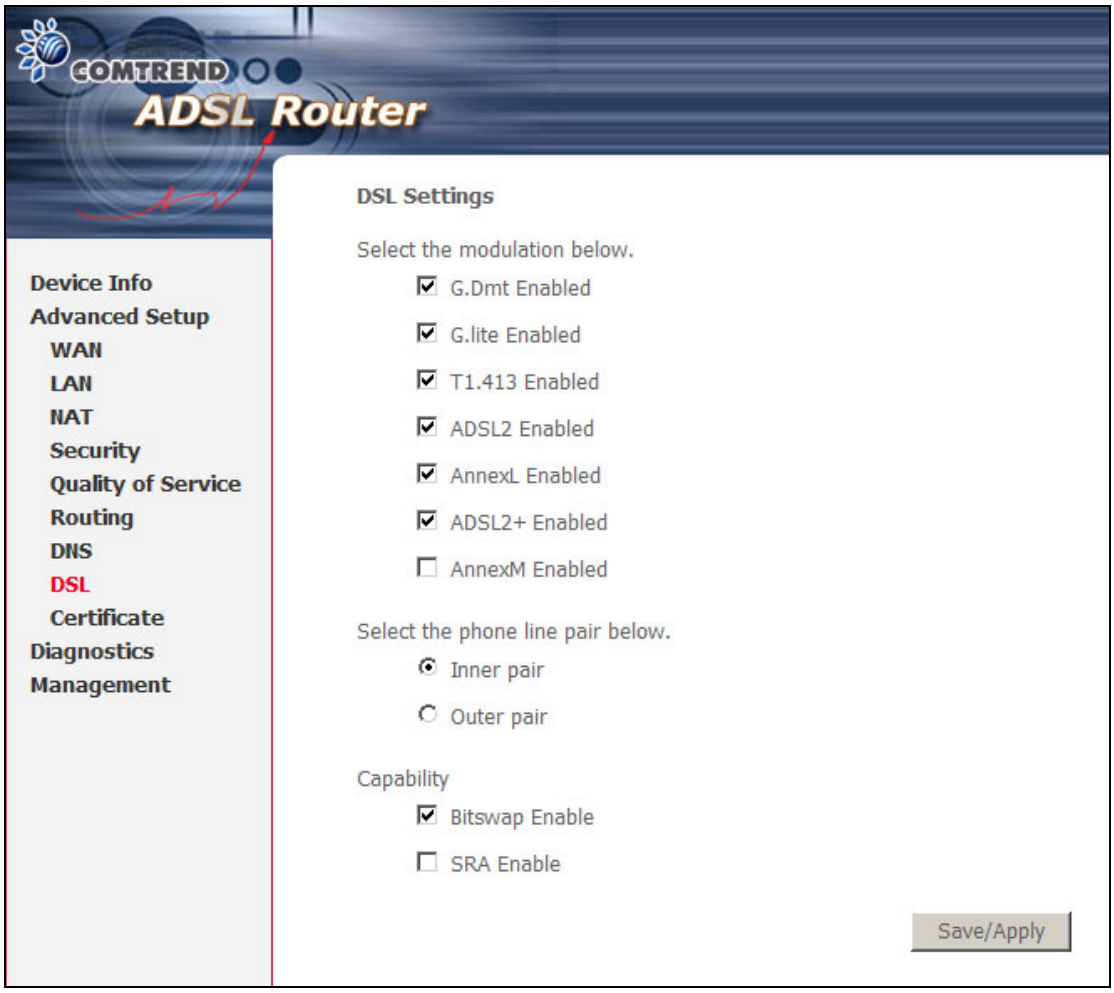
For dynamic DNS service, click the **Add** button. The following screen will display.



D-DNS provider	Select a dynamic DNS provider from the list
Hostname	Enter the name for the dynamic DNS server.
Interface	Select the interface from the list
Username	Enter the username for the dynamic DNS server.
Password	Enter the password for the dynamic DNS server.

6.8 DSL

To access the DSL settings, First click On **Advanced Setup** and then click on **DSL**. The DSL Settings dialog box allows you to select an appropriate modulation mode.

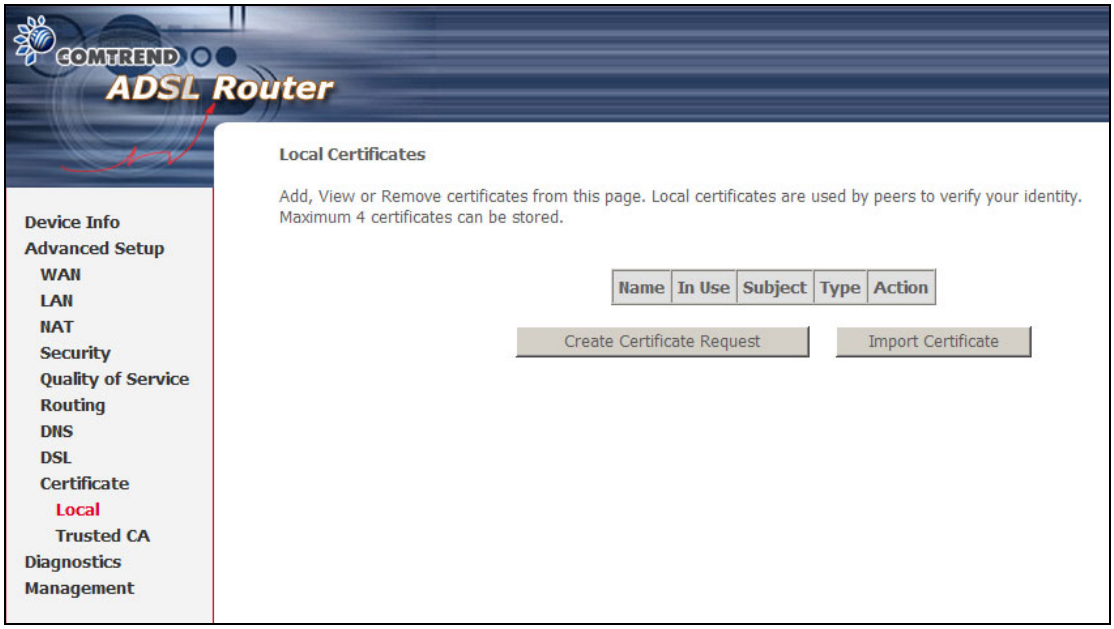


Option	Description
G.dmt Enabled	Sets G.Dmt if you want the system to use G.Dmt mode.
G.Lite Enabled	Sets G.Lite if you want the system to use G.Lite mode.
T1.413	Sets the T1.413 if you want the system to use only T1.413 mode.
ADSL2 Enabled	The device can support the functions of the ADSL2.
AnnexL Enabled	The device can support/enhance the long loop test.
ADSL2+ Enabled	The device can support the functions of the ADSL2+.
AnnexM	Covers a higher "upstream" data rate version, by making use of some of the downstream channels.
Inner Pair	Reserved only
Outer Pair	Reserved only
Bitswap Enable	Allows bitswapping function
SRA Enable	Allows seamless rate adaptation

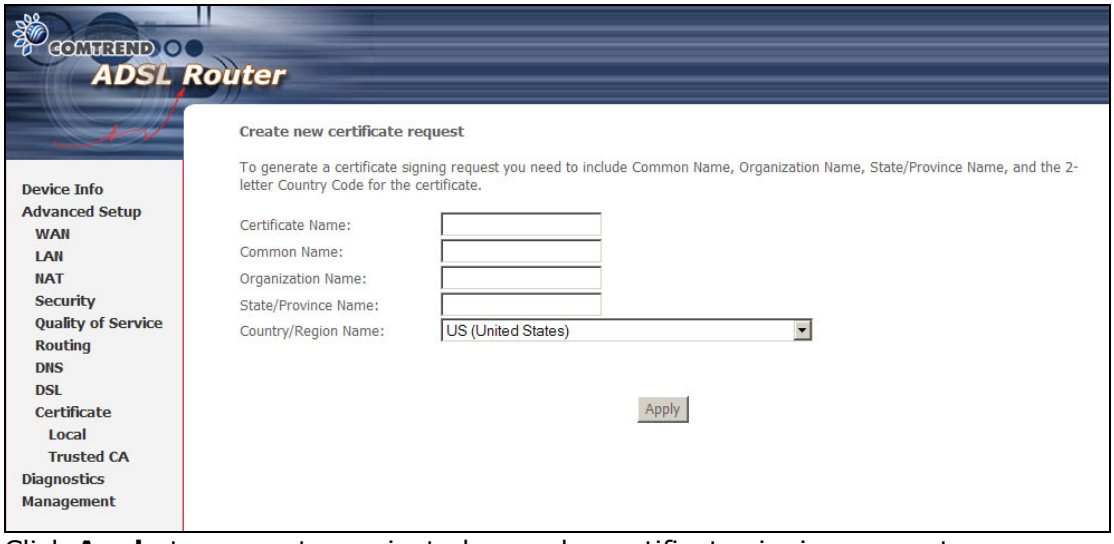
6.9 Certificate

A certificate is a public key, attached with its owner's information (company name, server name, personal real name, contact e-mail, postal address, etc) and digital signatures. There will be one or more digital signatures attached on the certificate, indicating that these signers have verified that the owner information of this certificate is correct.

6.9.1 Local



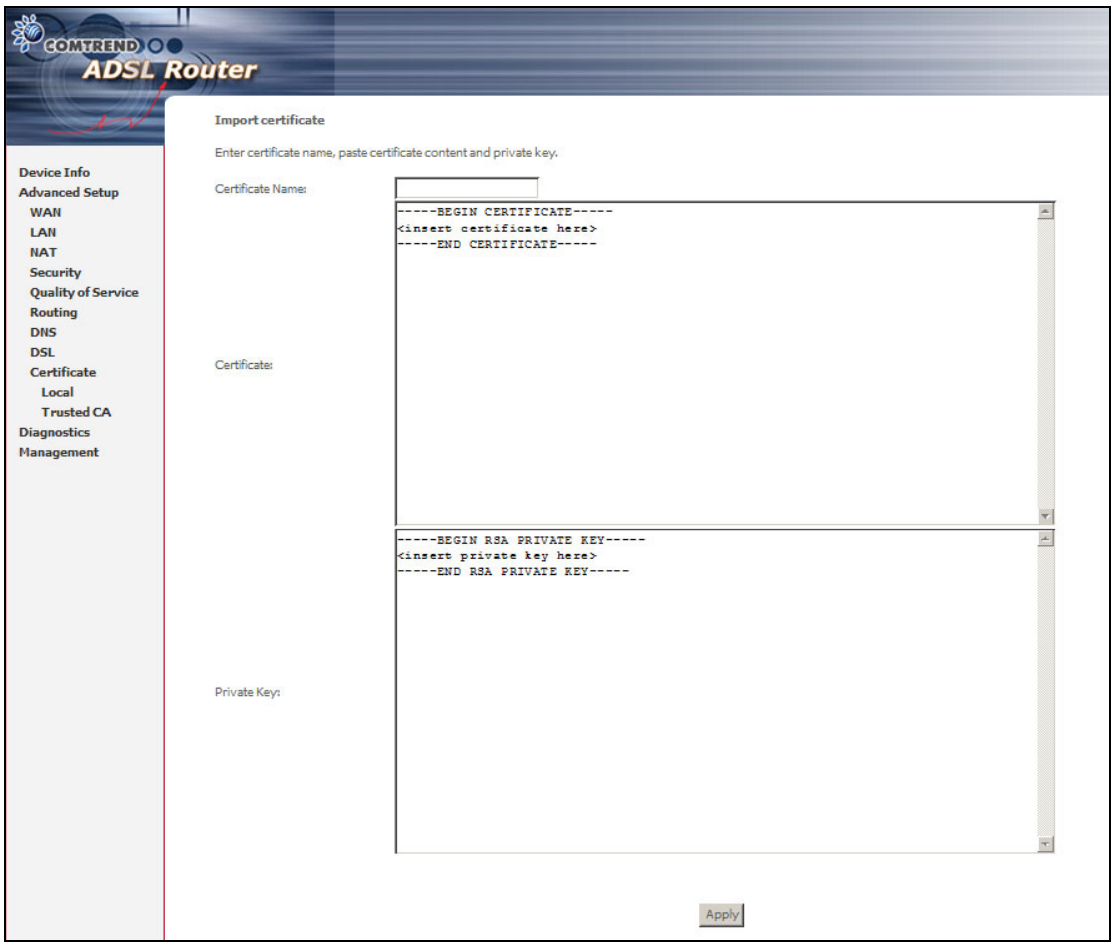
Click **Create Certificate Request** to generate a certificate signing request. The certificate signing request can be submitted to the vendor/ISP/ITSP to apply for a certificate. Some information must be included in the certificate signing request. Actually, your vendor/ISP/ITSP will ask you to provide the information they require and to provide the information in the format they regulate. The explanation for each column in the following table is only for reference.



Click **Apply** to generate a private key and a certificate signing request.

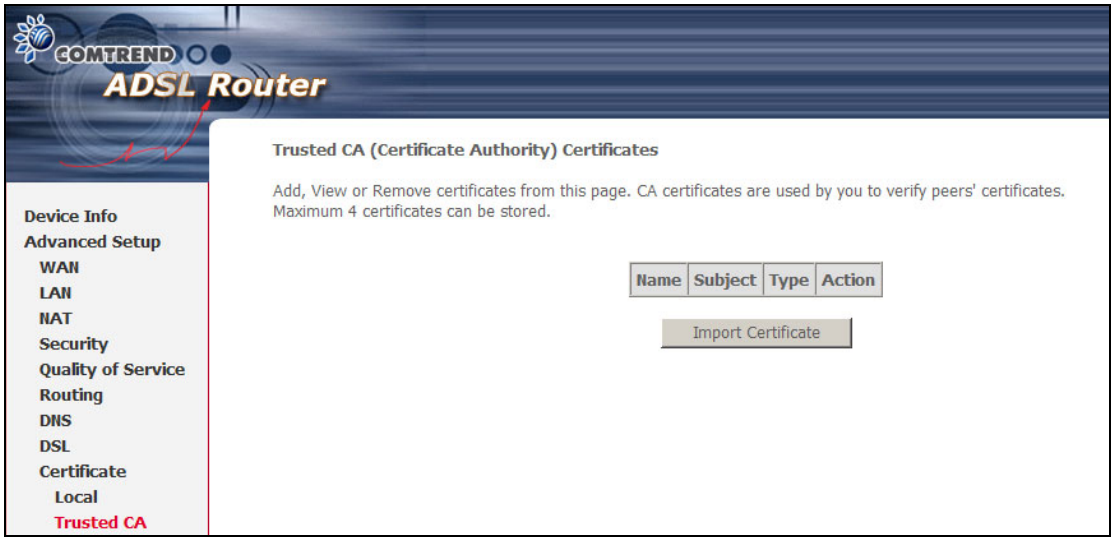
Certificate Name	A user-defined name for the certificate.
Common Name	Usually, it is the fully qualified domain name for the machine.
Organization Name	The exact legal name of your organization. Do not abbreviate.
State/Province Name	The state or province where your organization is located. It cannot be abbreviated.
Country/Region Name	The two-letter ISO abbreviation for your country.

This screen is used to paste the certificate content and the private key provided by your vendor/ISP/ITSP.

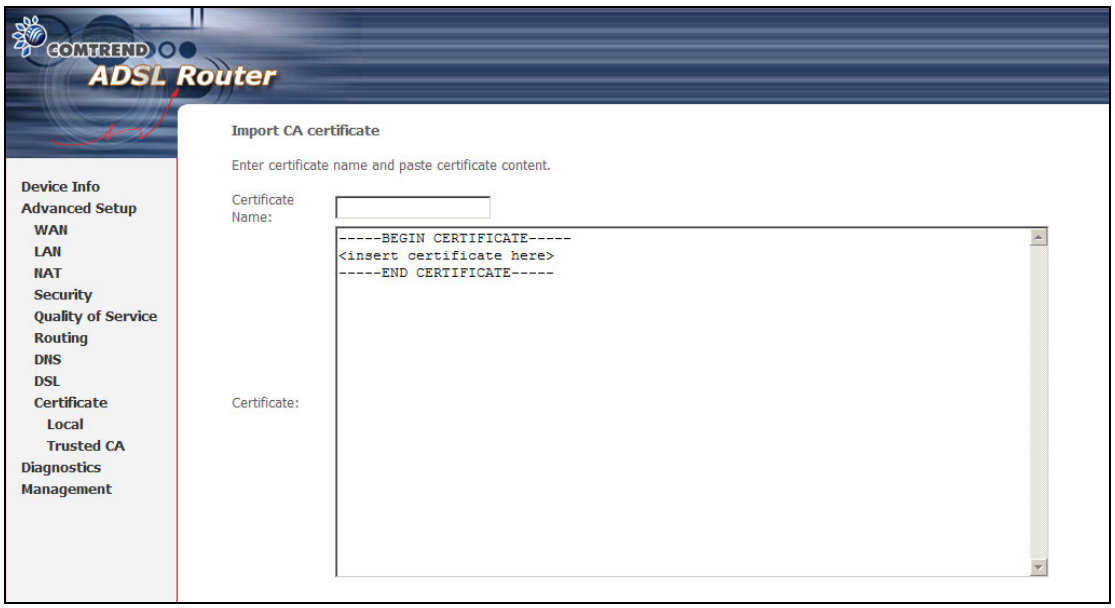


6.9.2 Trusted CA

CA is the abbreviation for Certificate Authority. CA is a part of the X.509 system. It is itself a certificate, attached with the owner information of this certificate authority. But its purpose is not to do encryption/decryption. Its purpose is to sign and issue certificates; in order to prove the owner information of that certificate is correct.

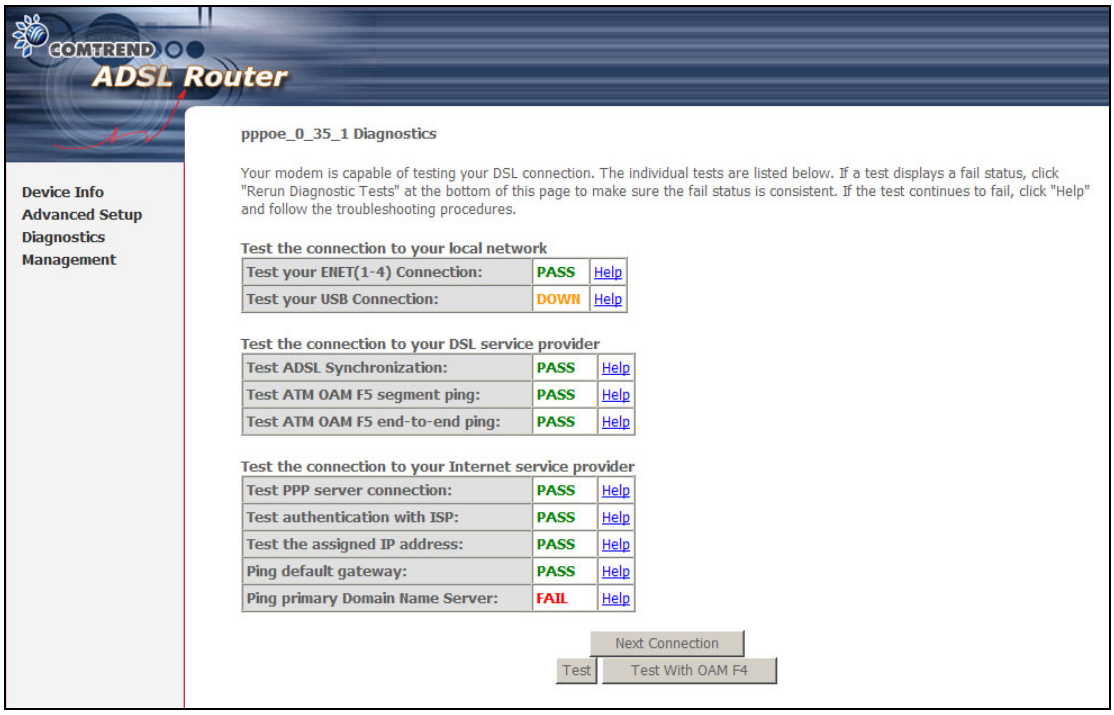


Click **Import Certificate** to paste the certificate content of your trusted CA. Generally speaking, the certificate content will be provided by your vendor / ISP / ITSP and is used to authenticate the Auto-Configuration Server (ACS) that the CPE will connect to.



Chapter 7 Diagnostics

The Diagnostics menu provides feedback on the connection status of the device. The individual tests are listed below. If a test displays a fail status, click **Rerun Diagnostic Tests** at the bottom of the screen to retest and confirm the error. If the test continues to fail, click **Help** and follow the troubleshooting procedures.


COMTREND
ADSL Router
Device Info
Advanced Setup
Diagnostics
Management
pppoe_0_35_1 Diagnostics
Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.
Test the connection to your local network
Test your ENET(1-4) Connection: PASS Help
Test your USB Connection: DOWN Help
Test the connection to your DSL service provider
Test ADSL Synchronization: PASS Help
Test ATM OAM F5 segment ping: PASS Help
Test ATM OAM F5 end-to-end ping: PASS Help
Test the connection to your Internet service provider
Test PPP server connection: PASS Help
Test authentication with ISP: PASS Help
Test the assigned IP address: PASS Help
Ping default gateway: PASS Help
Ping primary Domain Name Server: FAIL Help
Next Connection
Test
Test With OAM F4

The basic test set (no PVC configured) is described in the table below. For help with the other tests click on the **Help** link next to the test condition for guidance.

Test	**Condition**
ENET Connection	**Pass:** Indicates that the Ethernet interface on your computer is connected to the LAN port of this device. **Fail:** Indicates that the device does not detect the Ethernet interface on your computer.
USB connection	**Down**: Indicates that the device does not detect the USB interface on your computer. **NOTE:** This is not a problem however, since the CT-5611TC does not have a USB port.
ADSL Synchronization	**Pass:** Indicates that the DSL modem has detected a DSL signal from the telephone company. A solid ADSL LED on the device also indicates the detection of a DSL signal from the telephone company **Fail:** Indicates that the DSL modem does not detect a signal from the telephone company's DSL network. The ADSL LED will turn off.
Ping Default Gateway	**Pass:** Indicates that the device can communicate with the first entry point to the network. It is usually the IP address of the ISP local router. **Fail:** Indicates that the device was unable to communicate with the first entry point on the network. It may not have an effect on your Internet connectivity. Therefore, if this test fails but you are still able to access the Internet, there is no need to troubleshoot this issue.

Test	Condition
Ping Primary Domain Name Server	**Pass:** Indicates that the device can communicate with the primary Domain Name Server (DNS). **Fail:** Indicates that the device was unable to communicate with the primary Domain Name Server (DNS). It may not have an effect on your Internet connectivity. Therefore, if this test fails but you are still able to access the Internet, there is no need to troubleshoot this issue.

Chapter 8 Management

The Management section of the CT-5611TC supports the following maintenance functions and processes:

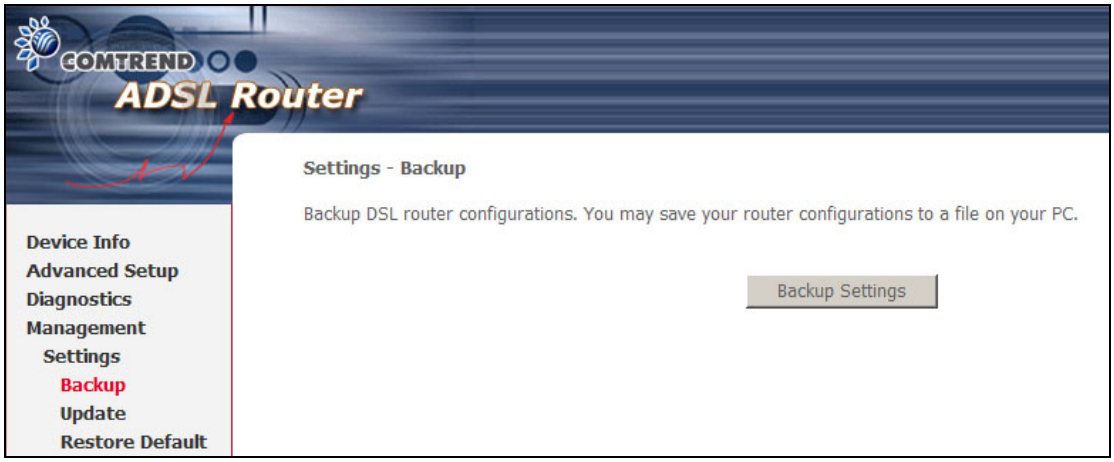
- Settings
- System log
- SNMP Agent
- TR-069 Client
- Internet Time
- Access Control
- Update Software
- Save/Reboot

8.1 Settings

The Settings option allows you to back up your settings to a file, retrieve the setting file, and restore the settings.

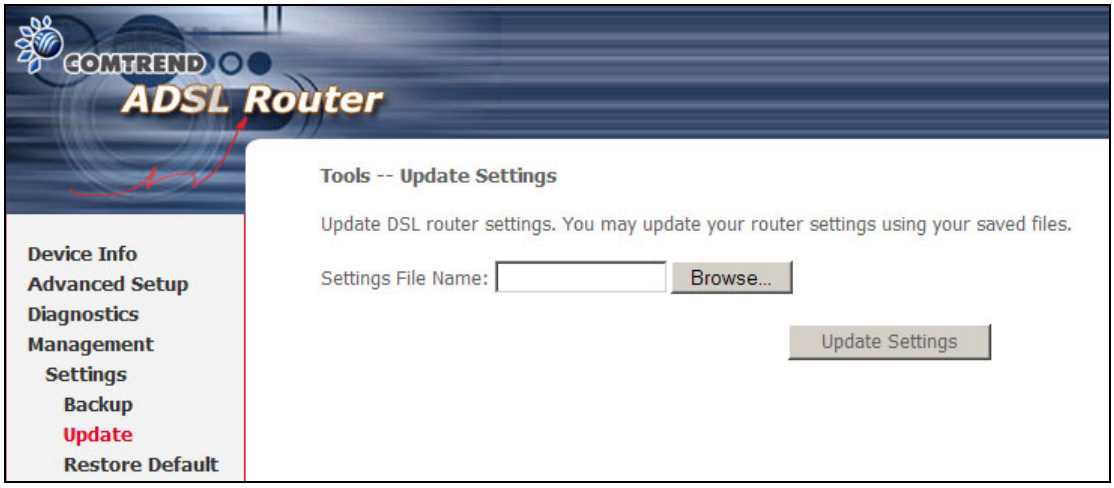
8.1.1 Backup Settings

The Backup option under Management>Settings, save your router configurations to a file on your PC. Click BACKUP Settings in the main window. You will be prompted to define the location of the backup file to save. After choosing the file location, click **Backup Settings.** Te file will then be saved to the assigned location.



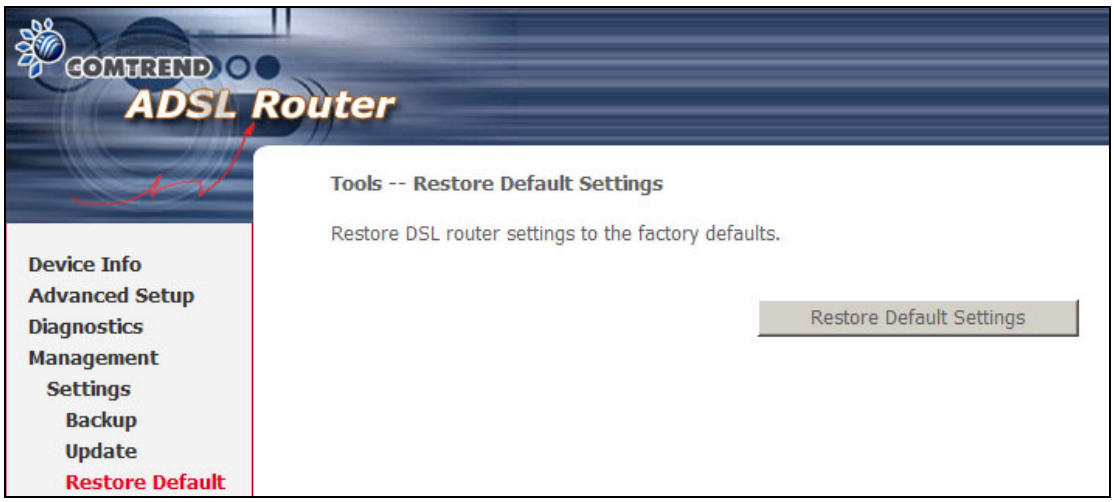
8.1.2 Update Settings

The Update option under Management>Settings update your router settings using your saved files.



8.1.3 Restore Default

Clicking the Restore Default Configuration option in the Restore Settings screen can restore the original factory installed settings.



After the Restore Default Configuration button is selected, the following screen appears. Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

DSL Router Restore

The DSL Router configuration has been restored to default settings and the router is rebooting.

Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

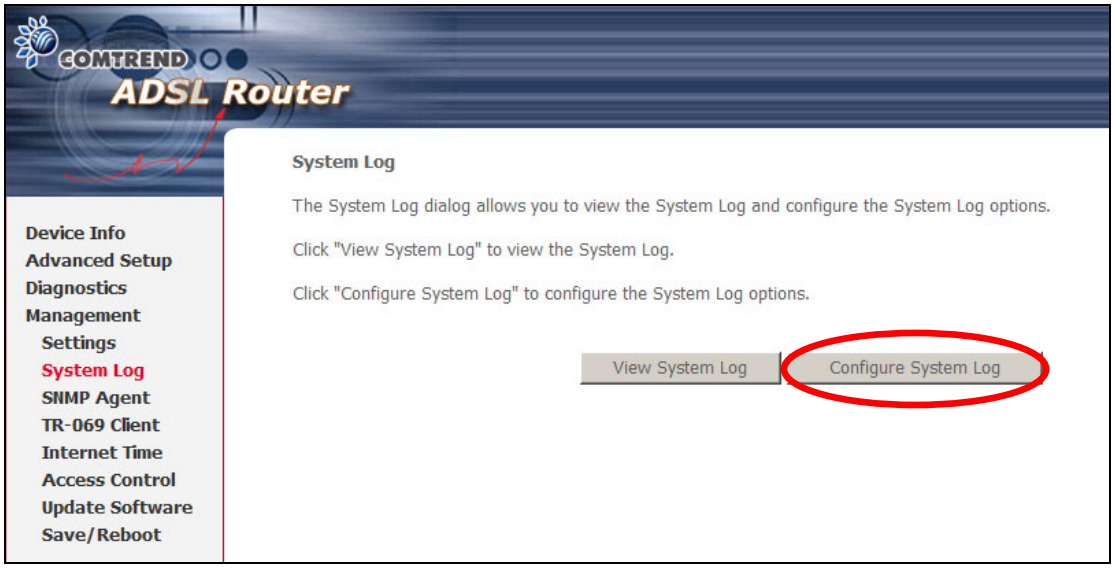
NOTE 1: This entry has the same effect as the hardware reset-to-default button. The CT-5611TC board hardware and the boot loader support the **reset to default** button. If the reset button is continuously pushed for more than 5 seconds, the boot loader will erase the entire configuration data saved on the flash memory.

NOTE 2: Restoring system settings, requires a system reboot. This necessitates that the current Web UI session be closed and restarted. Before restarting, the connected PC must be configured with a static IP address in the 192.168.1.x subnet in order to configure the CT-5611TC.

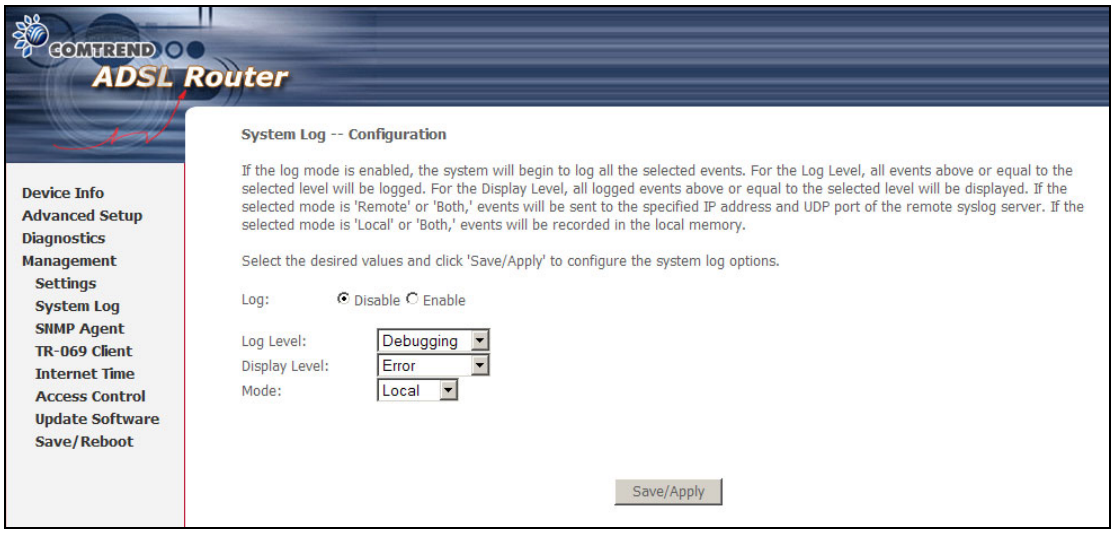
8.2 System Log

The System Log option under Management>Settings allows you to view the system events log, or to configure the System Log options. The default setting of system log is disabled. Follow the steps below to enable and view the system log.

Step 1: Click **Configure System Log** to display the following screen.

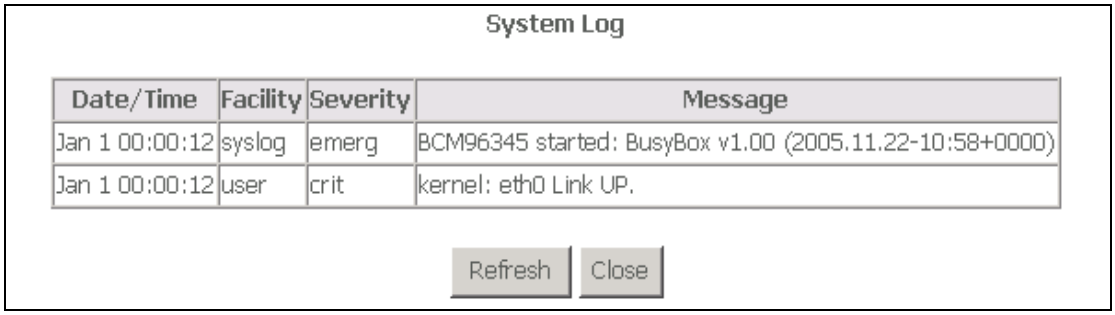


Step 2: Select desired options and then click **Save/Apply**.


COMTREND
ADSL Router
Device Info
Advanced Setup
Diagnostics
Management
Settings
System Log
SNMP Agent
TR-069 Client
Internet Time
Access Control
Update Software
Save/Reboot
System Log -- Configuration
If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.
Select the desired values and click 'Save/Apply' to configure the system log options.
Log: Disable Enable
Log Level: Debugging
Display Level: Error
Mode: Local
Save/Apply

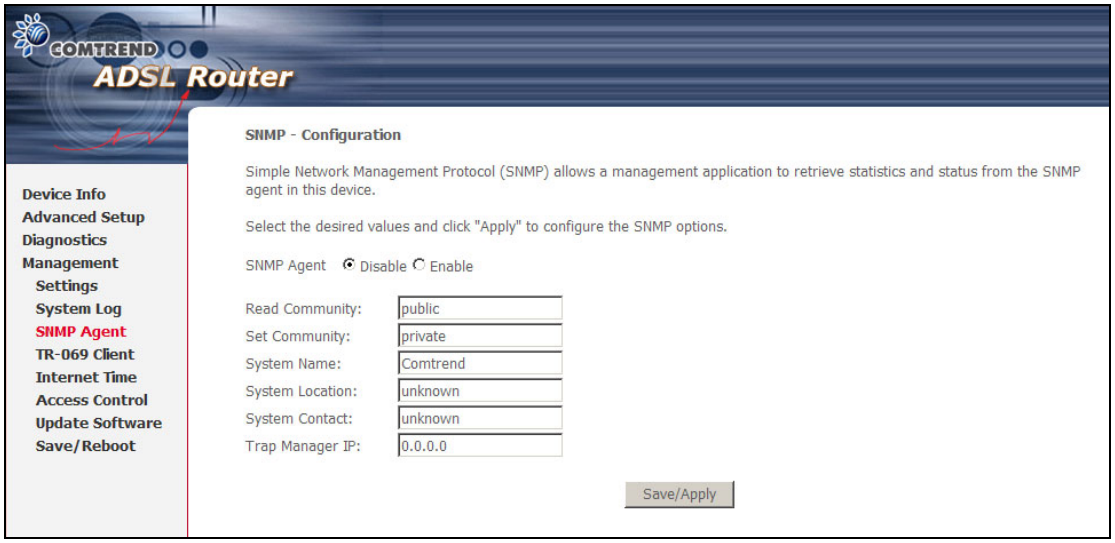
Option	Description
Log	Indicates whether the system is currently recording events. The user can enable or disable event logging. By default, it is disabled. To enable it, tick Enable and then Apply button.
Log level	Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the CT-5611TC SDRAM. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event. By default, the log level is "Debugging," which is the lowest critical level. The following log levels are • • • • • • • • Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.
Display Level	Allows the user to select the logged events and displays on the **View System Log** screen for events of this level and above to the highest Emergency level.
Mode	Allows you to specify whether events should be stored in the local memory, or be sent to a remote syslog server, or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote syslog server. When either Remote mode or Both mode is configured, the WEB UI will prompt the user to enter the Server IP address and Server UDP port.

3. Click **View System Log**. The results are displayed as follows.



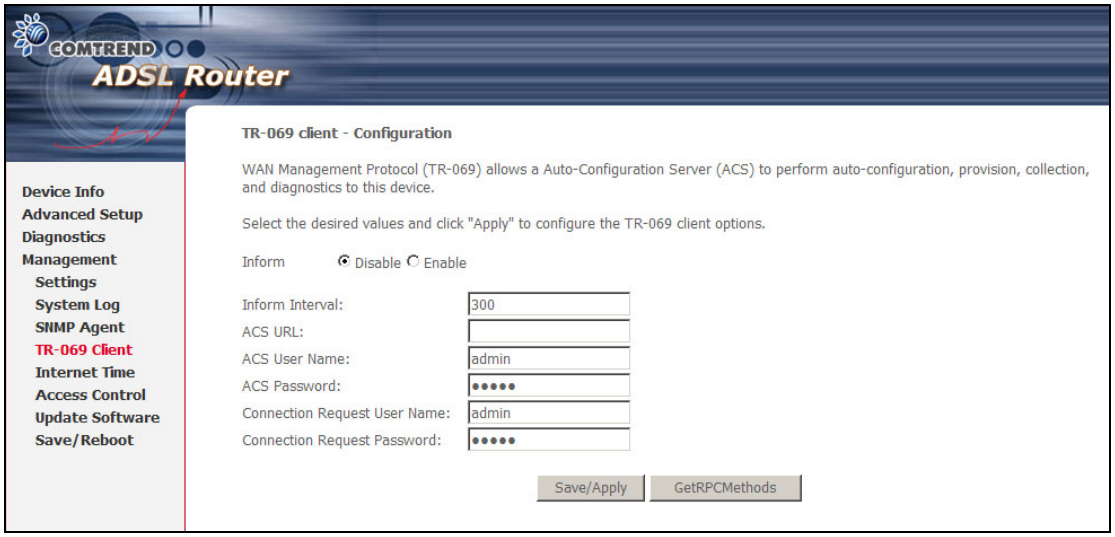
8.3 SNMP Agent

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device. Select the **Enable** radio button, configure options and click **Save/Apply** to activate SNMP.



8.4 TR-069 Client

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

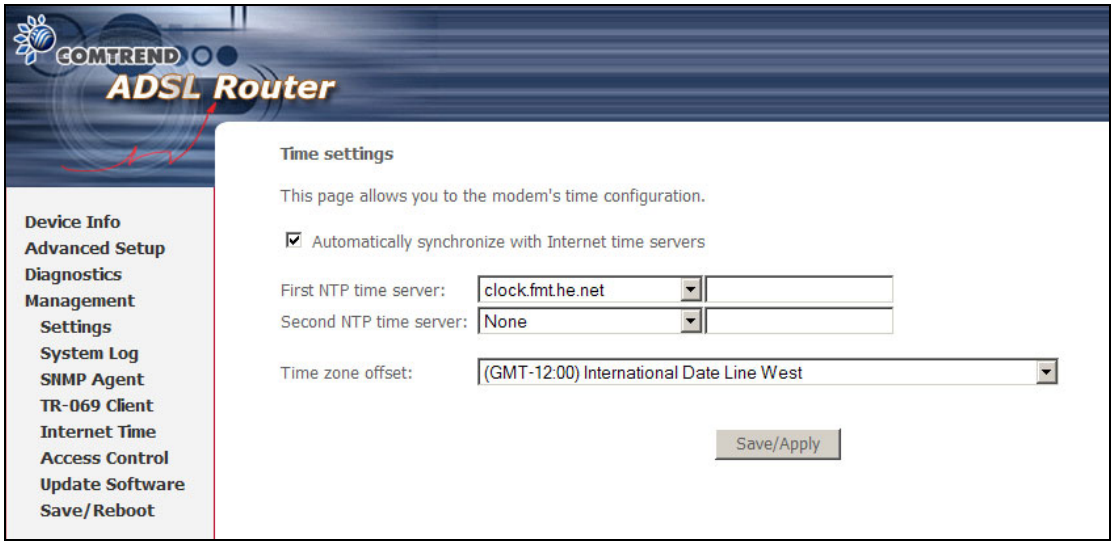


Option	Description
Inform	Disable/Enable TR-069 client on the CPE.
Inform Interval	The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the Inform method.
ACS URL	URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The "host" portion of this URL is

	used by the CPE for validating the certificate from the ACS when using certificate-based authentication.
ACS User Name	Username used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.
ACS Password	Password used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This password is used only for HTTP-based authentication of the CPE.
Connection Request User Name	Username used to authenticate an ACS making a Connection Request to the CPE.
Connection Request Password	Password used to authenticate an ACS making a Connection Request to the CPE.
Get RPC Methods	This method may be used by a CPE or ACS to discover the set of methods supported by the ACS or CPE it is in communication with. This list may include both standard TR-069 methods (those defined in this specification or a subsequent version) and vendor-specific methods. The receiver of the response MUST ignore any unrecognized methods. Click this button to force the CPE to immediately establish a connection to the ACS.

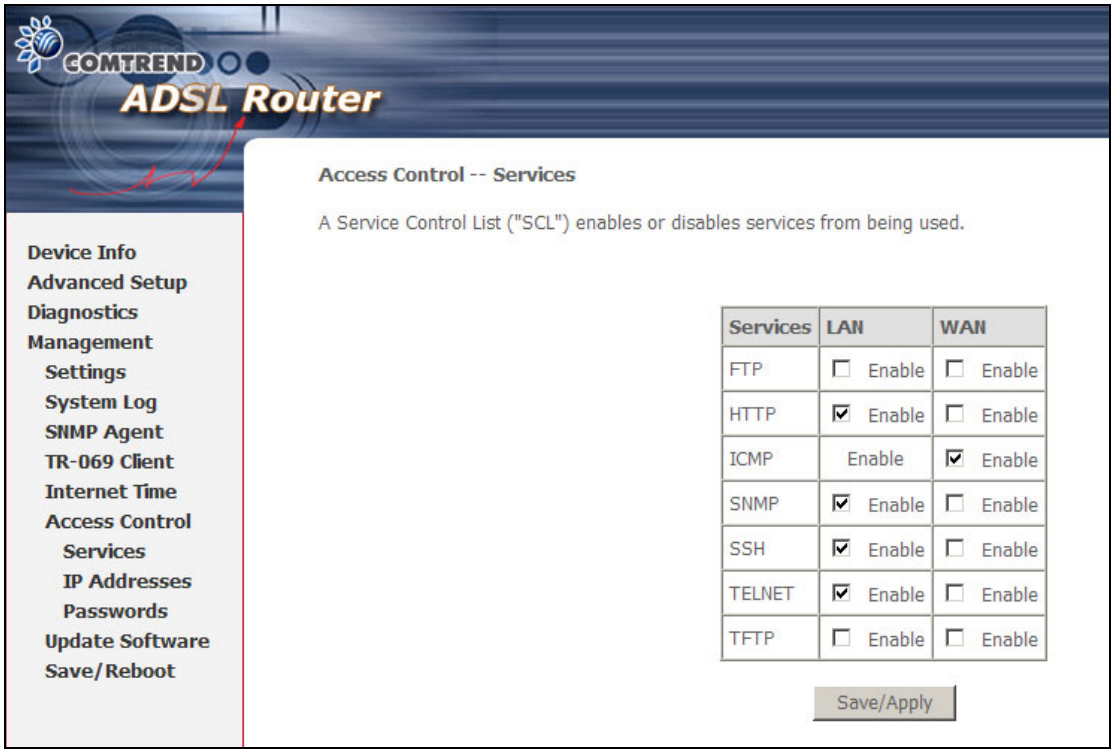
8.5 Internet Time

The Internet Time option under Management menu bar configures the Modem's time. To automatically synchronize with Internet timeservers, tick the corresponding box displayed on the screen. Then click **Save/Apply**.



8.6 Access Control

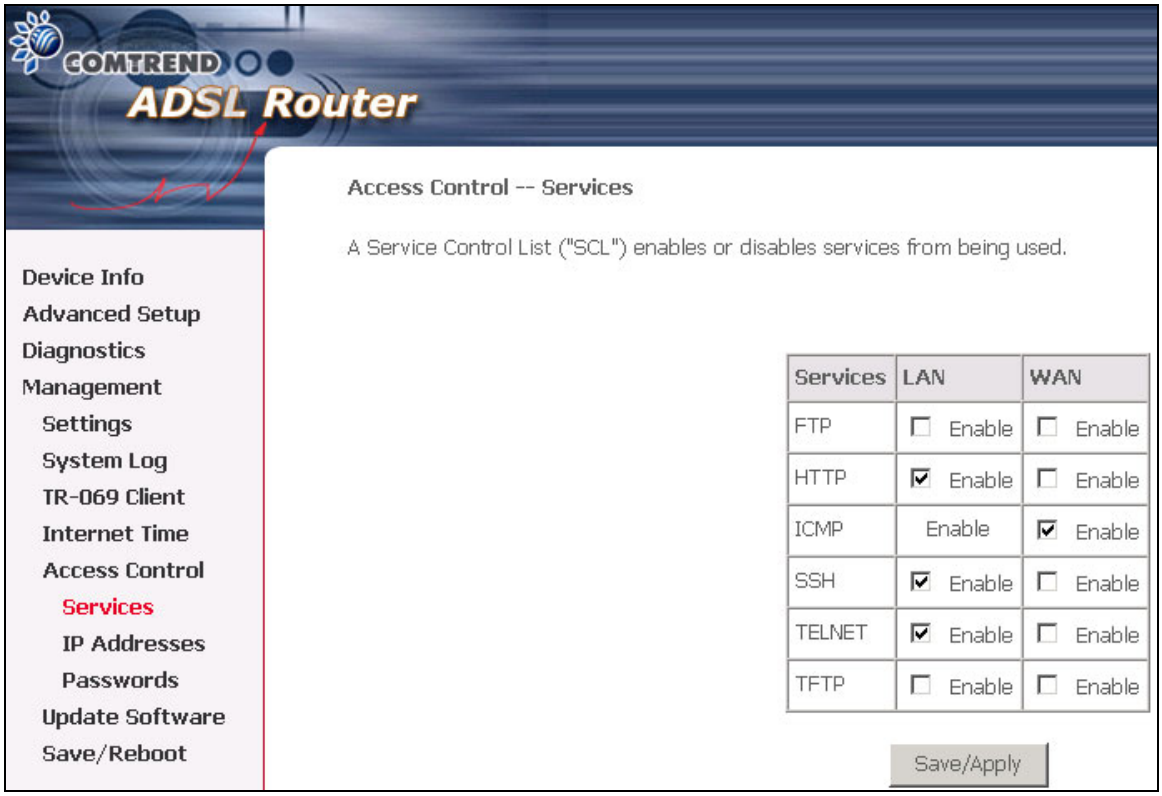
The Access Control option under Management menu bar configures the access-related parameters, including three parts: Services, IP Address, and Passwords.



Note: The WAN column is present only if the WAN interface is connected.

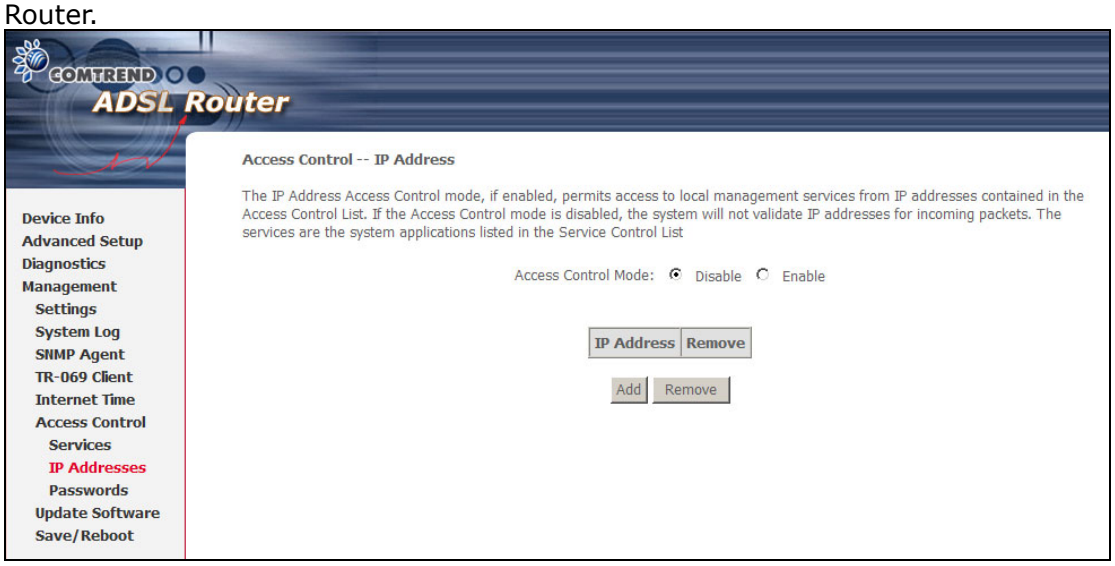
8.6.1 Services

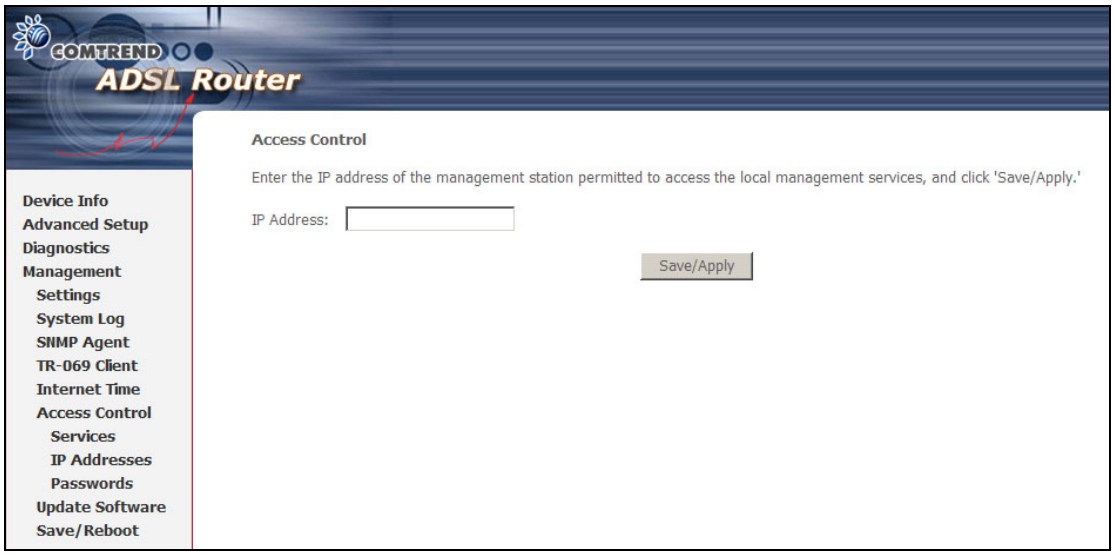
The Services option limits or opens the access services over the LAN or WAN. These services are provided FTP, HTTP, ICMP, SNMP, SSH (see Appendix C: SSH Client for details), TELNET, and TFTP. Enable the service by checking the item in the corresponding checkbox, and then click **Save/Apply**.



8.6.2 IP Addresses

The IP Addresses option limits the access by IP address. If the Access Control Mode is enabled, only the allowed IP addresses can access the router. Before you enable it, configure the IP addresses by clicking the **Add** button. Enter the IP address and click **Apply** to allow the PC with this IP address managing the DSL Router.



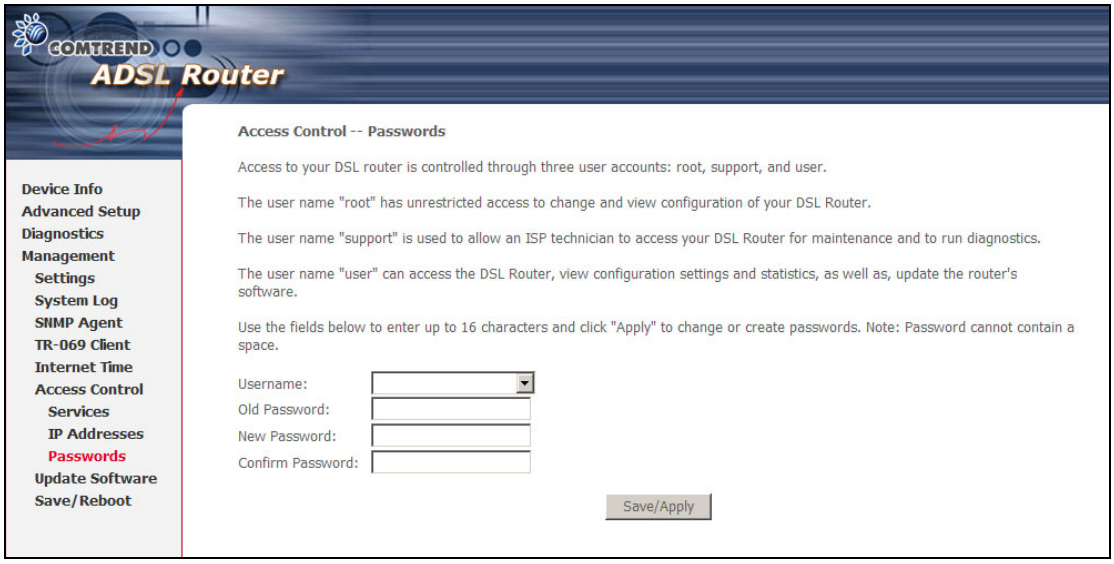


8.6.3 Passwords

The Passwords option configures the access passwords for the router. Access to your DSL router is controlled through three user accounts: admin, support, and user.

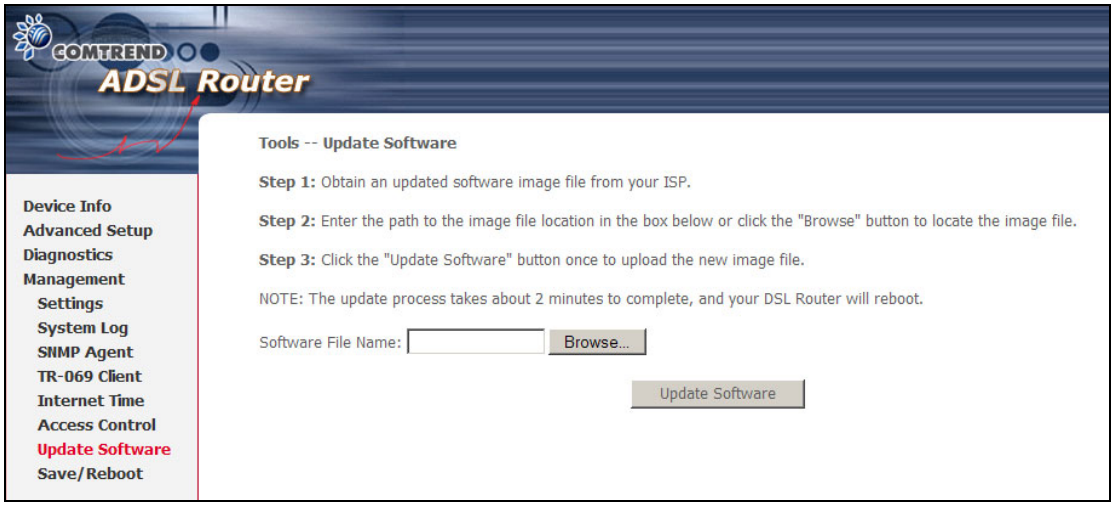
- **root** has unrestricted access to change and view the configuration.
- **support** is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.
- **user** can access the router, view configuration settings and statistics, as well as, update firmware.

Use the fields below to change password settings. Click **Save/Apply** to continue.


COMTREND
ADSL Router
Device Info
Advanced Setup
Diagnostics
Management
Settings
System Log
SNMP Agent
TR-069 Client
Internet Time
Access Control
Services
IP Addresses
Passwords
Update Software
Save/Reboot
Access Control -- Passwords
Access to your DSL router is controlled through three user accounts: root, support, and user.
The user name "root" has unrestricted access to change and view configuration of your DSL Router.
The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.
The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.
Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.
Username:
Old Password:
New Password:
Confirm Password:
Save/Apply

8.7 Update Software

The Update Software screen allows you to obtain an updated software image file from your ISP. Manual software upgrades from a locally stored file can be performed using the following screen.


COMTREND
ADSL Router
Device Info
Advanced Setup
Diagnostics
Management
Settings
System Log
SNMP Agent
TR-069 Client
Internet Time
Access Control
Update Software
Save/Reboot
Tools -- Update Software
Step 1: Obtain an updated software image file from your ISP.
Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.
Step 3: Click the "Update Software" button once to upload the new image file.
NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.
Software File Name:
Browse...
Update Software

Step 1: Obtain an updated software image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the **Browse** button to locate the image file.

Step 3: Click the "Update Software" button once to upload the new image file.

NOTE:	The update process takes about 2 minutes to complete, then DSL Router will reboot.

8.8 Save and Reboot

The Save/Reboot option saves the configurations and reboots the router. Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

Appendix A: Pin Assignments

Line port (RJ11)

Pin	Definition	Pin	Definition
1	-	4	ADSL_TIP
2	-	5	-
3	ADSL_RING	6	-

LAN Port (RJ45)

Pin	Definition	Pin	Definition
1	Transmit data+	5	NC
2	Transmit data-	6	Receive data-
3	Receive data+	7	NC
4	NC	8	NC

Appendix B: Specifications

Hardware Interface

RJ-11 X1 for ADSL2+, RJ-45 X 1 for LAN, mini-USB X 1 for LAN, Reset Button X 1, Power switch X 1

WAN Interface

Standard: ITU-T G.992.5, ITU-T G.992.3, ITU-T G.992.1, ANSI T1.413 Issue 2

G.992.5 (ADSL2+) .....Downstream : 24 Mbps Upstream : 1.3 Mbps
G.992.3 (ADSL2).....Downstream : 12 Mbps Upstream : 1.3 Mbps
G.DMT .....Downstream: 8 Mbps Upstream: 832 Kbps
Annex M

LAN Interface

Standard.....IEEE 802.3, IEEE 802.3u
10/100 BaseT .....Auto-sense
MDI/MDIX .....Yes

ATM Attributes

RFC 2364 (PPPoA), RFC 2684 (RFC 1483) Bridge/Route; RFC 2516 (PPPoE); RFC 1577 (IPoA)
Support PVCs 8
AAL type AAL5
ATM service class .....UBR/CBR/VBR
ATM UNI support.....UNI3.1/4.0
OAM F4/F5 .....Yes

Management

Compliant with remote management protocols TR-069/TR-098/TR-111, SNMP, SSH, Telnet, Web-based management, Configuration backup and restoration, Software upgrade via HTTP / TFTP / FTP server

Bridge Functions

Transparent bridging and learning .....IEEE 802.1d
Spanning Tree Algorithm .....Yes
IGMP Proxy .....Yes

Routing Functions

Static route, RIP v1/v2, NAT/PAT, DHCP Server/Relay/Client, DNS Proxy, ARP

Security Functions

Authentication protocols: PAP, CHAP, TCP/IP/Port filtering rules, Port Triggering/Forwarding, Packet and MAC address filtering, Access Control

QoS

L3 policy-based QoS, IP QoS, ToS

Application Passthrough

PPTP, L2TP, IPSec, VoIP, Yahoo messenger, ICQ, RealPlayer, NetMeeting, MSN, X-box, etc.

Power Supply

External power adapter.....110 Vac or 220 Vac

Environment Condition

Operating temperature .....0 ~ 50 degrees Celsius
Relative humidity .....5 ~ 95% (non-condensing)

Dimensions

152 mm (W) x 28 mm (H) x 112 mm (D)

Kit Weight

(1*CT-5611TC,1*RJ11 cable,1*USB cable,1*RJ45 cable,1*Power Adapter, *CD-ROM) = 0.65 kg

NOTE: Specifications are subject to change without notice

Appendix C: SSH Client

Linux OS has a ssh (Security Socket Share) client included. Although Microsoft Windows does not have a ssh client, there is a public domain one called "putty" that can be downloaded from here:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

To access the ssh client you must first enable SSH access for LAN or WAN from the Management → Access Control → Services menu in the web user interface.

To access the router using the Linux ssh client

For LAN access, type: ssh -l root 192.168.1.1

For WAN access, type: ssh -l support *WAN IP address*

To access the router using the Windows "putty" ssh client

For LAN access, type: putty -ssh -l root 192.168.1.1

For WAN access, type: putty -ssh -l support *WAN IP address*

NOTE:	The *WAN IP address* can be found on the Device Information → WAN menu screen.

Appendix D: Security

Stateful Packet Inspection
Refers to an architecture, where the firewall keeps track of packets on each connection traversing all its interfaces and makes sure they are valid. This is in contrast to static packet filtering which only examines a packet based on the information in the packet header.

Denial of Service Attack
Is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Various DoS attacks the device can withstand are ARP Attack, Ping Attack, Ping of Death, Land, SYN Attack, Smurf Attack, and Tear Drop.

TCP/IP/Port/Interface Filter
These rules help in the filtering of traffic at the Network layer i.e. Layer 3.
When a Routing interface is created, Enable Firewall must be checked.
Navigate to Advanced Setup -> Security -> IP Filtering.

Outgoing IP Filter
Helps in setting rules to DROP packets from the LAN interface. By default if Firewall is Enabled all IP traffic from LAN is allowed. By setting up one or more filters, particular packet types coming from the LAN can be dropped.

Filter Name: User defined Filter Name.

Protocol: Can take on any values from: TCP/UDP, TCP, UDP or ICMP

Source IP Address/Source Subnet Mask: Packets with the particular "Source IP Address/Source Subnet Mask" combination will be dropped.

Source Port: This can take on either a single port number or a range of port numbers. Packets having a source port equal to this value or falling within the range of port numbers (portX : portY) will be dropped.

Destination IP Address/Destination Subnet Mask: Packets with the particular "Destination IP Address/Destination Subnet Mask" combination will be dropped.

Destination Port: This can take on either a single port number or a range of port numbers. Packets having a destination port equal to this value or falling within the range of port numbers (portX : portY) will be dropped.

Example 1:

Filter Name	: Out_Filter1
Protocol	: TCP
Source Address	: 192.168.1.45
Source Subnet Mask	: 255.255.255.0
Source Port	: 80
Destination Address	: NA
Destination Subnet Mask	: NA
Destination Port	: NA

This filter will Drop all TCP packets coming from LAN with IP Address/Sub. Mask 192.168.1.45/24 having a source port of 80 irrespective of the destination. All other packets will be Accepted.

Example 2:

Filter Name	: Out_Filter2
Protocol	: UDP
Source Address	: 192.168.1.45
Source Subnet Mask	: 255.255.255.0
Source Port	: 5060:6060
Destination Address	: 172.16.13.4
Destination Subnet Mask	: 255.255.255.0
Destination Port	: 6060:7070

This filter will drop all UDP packets coming from LAN with IP Address/ Subnet Mask 192.168.1.45/24 and a source port in the range of 5060 to 6060, destined to 172.16.13.4/24 and a destination port in the range of 6060 to 7070.

Incoming IP Filtering:
Helps in setting rules to ACCEPT packets from the WAN interface. By default, all incoming IP traffic from the WAN is Blocked, if the Firewall is Enabled. By setting up one or more filters, particular packet types coming from the WAN can be Accepted.

Filter Name: User defined Filter Name.

Protocol: Can take on any values from TCP/UDP, TCP, UDP or ICMP

Source IP Address/Source Subnet Mask: Packets with the particular "Source IP Address/Source Subnet Mask" combination will be accepted.

Source Port: This can take on either a single port number or a range of port numbers. Packets having a source port equal to this value or falling within the range of port numbers (portX : portY) will be accepted.

Destination IP Address/Destination Subnet Mask: Packets with the particular "Destination IP Address/Destination Subnet Mask" combination will be accepted.

Destination Port: This can take on either a single port number or a range of port numbers. Packets having a destination port equal to this value or falling within the range of port numbers (portX : portY) will be accepted.

The WAN interface on which these rules apply needs to be selected by user.

Example 1:

Filter Name	: In_Filter1
Protocol	: TCP
Source Address	: 210.168.219.45
Source Subnet Mask	: 255.255.0.0
Source Port	: 80
Destination Address	: NA
Destination Submask	: NA
Destination Port	: NA

Selected WAN interface: mer_0_35/nas_0_35

This filter will ACCEPT all TCP packets coming from WAN interface mer_0_35/nas_0_35 with IP Address/Sub. Mask 210.168.219.45/16 having a

source port of 80 irrespective of the destination. All other incoming packets on this interface are DROPPED.

Example 2:

Filter Name	: In_Filter2
Protocol	: UDP
Source Address	: 210.168.219.45
Source Subnet Mask	: 255.255.0.0
Source Port	: 5060:6060
Destination Address	: 192.168.1.45
Destination Subnet Mask	: 255.255.255.0
Destination Port	: 6060:7070

This rule will ACCEPT all UDP packets coming from WAN interface mer_0_35/nas_0_35 with IP Address/Subnet Mask 210.168.219.45/16 and a source port in the range of 5060 to 6060, destined to 192.168.1.45/24 and a destination port in the range of 6060 to 7070. All other incoming packets on this interface are DROPPED.

MAC Layer Filtering: These rules help in the filtering of traffic at the Layer 2. MAC Filtering is only effective on ATM PVCs configured in Bridge mode. After a Bridge mode PVC is created, navigate to Advanced Setup - Security - MAC Filtering.

Global Policy: When set to Forwarded the default filter behavior is to Forward all MAC layer frames except those explicitly stated in the rules. Setting it to Blocked changes the default filter behavior to Drop all MAC layer frames except those explicitly stated in the rules.

Protocol Type: Either PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP.

Destination MAC Address: Of the form, XX:XX:XX:XX:XX:XX. Frames with this particular destination address will be Forwarded/Dropped depending on whether the Global Policy is Blocked/Forwarded.

Source MAC Address: Of the form, XX:XX:XX:XX:XX:XX. Frames with this particular source address will be Forwarded/Dropped depending on whether the Global Policy is Blocked/Forwarded.

Frame Direction: (User must select interface on which this rule is applied)

LAN <=> WAN --> All Frames coming/going to/from LAN or to/from WAN.
WAN => LAN --> All Frames coming from WAN destined to LAN.
LAN => WAN --> All Frames coming from LAN destined to WAN

Example 1:

Global Policy: Forwarded
Protocol Type: PPPoE
Destination MAC Address: 00:12:34:56:78:90
Source MAC Address: NA
Frame Direction: LAN => WAN
WAN Interface Selected: br_0_34/nas_0_34

Addition of this rule drops all PPPoE frames going from LAN-side to WAN-side with a Destination MAC Address of 00:12:34:56:78:90 irrespective of its Source MAC Address on the br_0_34 WAN interface. All other frames on this interface are forwarded.

Example 2:

Global Policy: Blocked
Protocol Type: PPPoE
Destination MAC Addr: 00:12:34:56:78:90
Source MAC Addr: 00:34:12:78:90:56
Frame Direction: WAN => LAN
WAN Interface Selected: br_0_34/nas_0_34

Addition of this rule forwards all PPPoE frames going from WAN-side to LAN-side with a Destination MAC Address of 00:12:34:56:78 and Source MAC Address of 00:34:12:78:90:56 on the br_0_34 WAN interface. All other frames on this interface are dropped.

Daytime Parental Control
This feature restricts access of a selected LAN device to an outside Network through the device, as per chosen days of the week and the chosen times.

User Name: Name of the Filter.

Browser MAC Address: Displays MAC address of the LAN device on which the browser is running.

Other MAC Address: If restrictions are to be applied to a device other than the one on which the browser is running, the MAC address of that LAN device is entered.

Days of the Week: Days of the week, when the restrictions are applied.

Start Blocking Time: The time when restrictions on the LAN device begin.

End Blocking Time: The time when LAN device restrictions are lifted.

Example:

User Name: FilterJohn
Browser's MAC Address: 00:25:46:78:63:21
Days of the Week: Mon, Wed, Fri
Start Blocking Time: 14:00
End Blocking Time: 18:00

When this rule i.e. FilterJohn is entered, a LAN device with MAC Address of 00:25:46:78:63:21 will be restricted access to the outside network on Mondays, Wednesdays, and Fridays, from 2pm to 6pm. On all other days and time, this device will have access to the outside Network.